2001

Criminal Law in Cyberspace

Neal K. Katyal
Georgetown University Law Center, katyaln@law.georgetown.edu

149 U. Pa. L. Rev. 1003 (2000-2001)

CRIMINAL LAW IN CYBERSPACE

NEAL KUMAR KATYAL†

---

† Associate Professor of Law, Georgetown University Law Center. Thanks to Bruce Ackerman, Akhil Amar, Fred Cohen, Julie Cohen, Dhammika Dharmapala, Michael Froomkin, Jennifer Granick, Julie Hilden, Adam Isles, Jerry Kang, Sonia Katyal, Gillian Lester, Josh Liston, Wayne Mink, Wendy Perdue, Mark Rasch, Jeffrey Rosen, Joanna Rosen, Jonathan Rusch, Warren Schwartz, Mike Seidman, Anna Selden, Andrew Shapiro, Neal Stephenson, Cliff Stoll, Lynn Stout, Mark Tushnet, Eugene Volokh, and participants in a Georgetown University Faculty Workshop.

INTRODUCTION

The new millennium brings new crimes. Witness two of the most talked-about crimes of last year, the ILoveYou computer worm (in terms of economic damage, perhaps the most devastating crime in history, causing more than $11 billion in losses) and the denial-of-service attacks on Yahoo!, eBay, E*Trade, and other sites (which caused $1.2 billion in damage).[1] These events suggest that a new breed of crime has emerged over the past decade: cybercrime. This umbrella term covers all sorts of crimes committed with computers—from viruses to Trojan horses; from hacking into private e-mail to undermining defense and intelligence systems; from electronic thefts of bank accounts to disrupting web sites. Law has not necessarily caught up with these crimes, as the recent dismissal of charges against the author of the ILoveYou worm demonstrates.[2] How should the law think about computer crime?

Some academics see cyberspace as a new area in which first principles of law need to be rethought. David Johnson and David Post, for example, contend that existing legal rules are not suitable for the digital age and that governments should not necessarily impose legal order on the internet.[3] Others, in contrast, believe that a

---

[1] Russ Banham, *Hacking It*, CFO MAG., Aug. 1, 2000, http://www.cfo.com/printarticle/1,1883,0|1|AD|874,00.html (describing the denial of service attacks as "causing more than $1.2 billion in total losses"); Harvey Stark, *eVirus Signs Marketing and Sales Contract and Readies for Expansion*, BUS. WIRE, Aug. 1, 2000, 8/1/00 BWIRE 09:21:00 ("[T]he 'I Love You' virus caused estimated damages of US$11 billion worldwide in May, 2000.").

[2] *See Philippines Drops Charges in "ILoveYou" Virus Case, at* http://www.cnn.com/2000/TECH/computing/08/21/computers.philippines.reut/index.html (Aug. 21, 2000).

[3] *See* David R. Johnson & David G. Post, *And How Shall the Net Be Governed?: A Meditation on the Relative Virtues of Decentralized, Emergent Law, in* COORDINATING THE INTERNET 62, 68 (Brian Kahin & James H. Keller eds., 1997) (proposing a model for internet governance based on "decentralized, emergent law" stemming from the "voluntary acceptance of standards"); David R. Johnson & David Post, *Law and*

computer is merely an instrument and that crime in cyberspace should be regulated the same way as criminal acts in realspace.[4] The recent U.S. Department of Justice ("DOJ") report on cybercrime typifies this approach.[5] I contend that neither view is correct and that each camp slights important features that make cybercrime both different from and similar to traditional crime.

Underlying the "cybercrime is not different" position is a worry about a unique form of geographic substitution. The concern is that disproportionately punishing activity in either realspace or cyberspace will induce criminals to shift their activities to that sphere in which the expected punishment is lower. For example, if the electronic theft of one million dollars warrants five years imprisonment, and the physical theft of one million dollars warrants ten years imprisonment,

---

Borders—The Rise of Law in Cyberspace, 48 STAN. L. REV. 1367, 1372-75 (1996); *see also* Benjamin Wittes, *Is Law Enforcement Ready for Cybercrime?*, LEGAL TIMES, Oct. 10, 1994, at 1 (discussing how some describe the internet as "'qualitatively different' from other platforms for crime" and how others, such as Stewart Baker, former general counsel at the National Security Agency, believe that such a characterization is "broadly speaking—wrong").

[4] *See, e.g.*, Catherine Thérèse Clarke, *From CrimINet to Cyber-Perp: Toward an Inclusive Approach to Policing the Evolving Criminal Mens Rea on the Internet*, 75 OR. L. REV. 191, 204-05 (1996) (discussing an informal survey of lawyers revealing that "most lawyers consider criminals on the 'net to be exactly the same as those outside the 'net"); Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998) (arguing that cyberspace can be regulated in many traditional ways); Christopher M. Kelly, *The Cyberspace Separatism Fallacy*, 34 TEX. INT'L L.J. 413, 414 (1999). In an important middle approach, Larry Lessig contends that cyberspace can be regulated through law and programming code. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 53-60 (1999).

Some courts have also suggested that crimes might be different in cyberspace because there is a lack of tangible media, such as a briefcase that may be "stolen." *See, e.g.*, United States v. Carlin Communications, Inc., 815 F.2d 1367, 1371 (10th Cir. 1987) (declining to apply the federal obscenity statute to abusive or harassing phone calls because such calls do not constitute "tangible objects" of commerce). Others have disagreed. *See* United States v. Thomas, 74 F.3d 701, 707 (6th Cir. 1996) (concluding that computer image files are tangible and therefore subject to the federal obscenity statute); United States v. Gilboe, 684 F.2d 235, 238 (2d Cir. 1982).

[5] The Justice Department believes that "substantive regulation of unlawful conduct . . . should, as a rule, apply in the same way to conduct in the cyberworld as it does to conduct in the physical world. If an activity is prohibited in the physical world but not on the Internet, then the Internet becomes a safe haven for that unlawful activity." U.S. DEPT. OF JUSTICE, THE ELECTRONIC FRONTIER: THE CHALLENGE OF UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET 11 (2000), *available at* http://www.usdoj.gov/criminal/cybercrime/unlawful.htm [hereinafter DOJ REPORT]. Current federal law, in general, embraces the view that there are no differences. *See id.* at vi ("[E]xisting substantive federal laws generally do not distinguish between unlawful conduct committed through the use of the Internet and the same conduct committed through the use of other, more traditional means of communication.").

criminals are likely to opt for the electronic theft. Such analysis is, however, incomplete. Beccaria and Becker have observed that the expected penalty for criminal activity is not only the sentence in the criminal code, but also a function of the probability that one will get caught.[6] To the extent that cybercrimes are easier to get away with, sentences might be increased to compensate for this lower probability.

In addition to the probability of being caught, another variable overlooked by the "cybercrime is not different" camp is the perpetration cost of engaging in crime. A bank robbery in realspace, for example, consumes tremendous criminal resources. A robber has to hire lookouts and firepower, garner inside knowledge about the bank, and so on. Profits will be split among five, six, or even more people. A computer theft, by contrast, involves fewer resources and may even be accomplished by a single person sitting down at a computer. Because cybercrime requires fewer resource inputs and less investment to cause a given level of harm, the law might approach these crimes differently.

These variations suggest that cyberspace is a unique medium for three reasons. *First*, and most importantly, the use of computers and other equipment is a cheaper means to perpetrate crime. Criminal law must be concerned not only with punishing crime ex post, but with creating ex ante barriers to inexpensive ways of carrying out criminal activity. In this Article, this principle—which is generally applicable in criminal law—will be called "cost deterrence." The idea is that law should strive to channel crime into outlets that are more costly to criminals. Cyberspace presents unique opportunities for criminals to reduce their perpetration costs; the probability of success in inflicting a certain level of harm while holding expenditures constant is greater. Accordingly, the law should develop mechanisms to neutralize these efficiency advantages.

Some neutralization techniques, however, risk punishing utility-producing activities. For example, encryption has the potential to further massive terrorism (which leads many in the law enforcement community to advocate its criminalization) but also has the potential to facilitate greater security in communication and thereby encourage freedom (which leads many others to push for unfettered access to the technology). This is a standard dilemma that the law encounters

---

[6] Cesare Beccaria, *On Crimes and Punishments, in* ON CRIMES AND PUNISHMENTS AND OTHER WRITINGS 1, 43, 57, 58 (Richard Bellamy ed., Richard Davies et al. trans., Cambridge Univ. Press 1995) (1764); Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169, 176 (1968).

in the regulation of technology—call it the "dual-use problem." The problem arises when an activity has both positive and negative uses and forbidding the act forfeits the good uses. To help solve the problem, I introduce a conventional tool, the sentencing enhancement, as a mechanism that can selectively target improper uses. Policymakers and academics have given little attention to sentencing enhancements and lack a theory of when they should be used. This Article endeavors to fill that gap, arguing that sentencing enhancements are suited to certain acts that are not inherently harmful to society and whose benefits depend on context. It shows, for example, how enhancements provide a solution to the encryption debate because they can be aimed at encryption's harmful applications.

Second, cybercrime adds additional parties to the traditional perpetrator-victim scenario of crime. In particular, much cybercrime is carried out through the use of Internet Service Providers ("ISPs"), such as America Online. Government should consider imposing responsibilities on such third parties because doing so promotes cost deterrence. Third parties can develop ways to make criminal activity more expensive and may be able to do so in ways that the government cannot accomplish directly. The same logic sometimes can apply to victims of cybercrime; law can develop mechanisms to encourage optimal victim behavior as well. As part of this discussion, this Article shows how victim self-help depends on changing police behavior and outlines a strategy to make police departments behave more like fire departments (focusing more on warning and prevention and less on chasing suspected perpetrators after they commit crimes).

Two features of cyberspace, however, suggest that these burden-shifting strategies will be difficult to implement. The first, which borrows from the New Economy theory of "network effects," contends that interconnectivity is an important goal that should not be sacrificed lightly. If potential victims and third parties like ISPs are forced to take precautionary measures—from building strong firewalls to forgoing communication with risky computer systems—these measures may diminish the value of the internet. A strong public law enforcement presence is necessary to prevent the net from fragmenting into small regions accessible only to subsets of trusted users with the right passkeys. A second feature that limits burden-shifting arises from the asymmetric incentives between ISPs and their users. Because an ISP derives little utility from providing access to a risky subscriber, a legal regime that places liability on an ISP for the

acts of its subscribers will quickly lead the ISP to purge risky ones from its system. ISPs, as private entities, face no constitutional constraints and little public accountability; the results of ISP liability may be unfair and threaten the potential benefits of the net.

Third, and more generally, a host of thorny problems arise because most activities that occur in cyberspace are invisible to third parties—and sometimes even to second parties. In a space where crimes are invisible, strategies that focus on trying to prevent crime by maintaining public order, such as "broken windows" policing, are of limited utility (though some insights can be adapted to cyberspace). Social norms cannot operate as effectively to prevent crime on the net because its users are not necessarily constrained by the values of realspace.

On the other side of the ledger, the danger of overly aggressive law enforcement is multiplied in cyberspace. Each new major cybercrime leads law enforcement to push for changes to the technical infrastructure to create better monitoring and tracing. If these monitoring mechanisms are hidden in private hardware and software, however, some contend that public accountability may be undermined. A similar point can be made about enforcement by police: Because police are invisible on the internet, the potential for entrapment or other forms of police misconduct may be greater. The ultimate effect of this loss of police visibility may be to poison legitimate activity on the net because confidence in communication may be undermined. An internet user will not be sure that he is talking to a friend and not a government interloper seeking evidence of criminal activity.[7] Because the technology of law enforcement is not well understood among the public, citizens will fear the net and its potential advantages will be stymied. Consider the public uproar over a third prominent news item from this year: the discovery that the Federal Bureau of Investigation ("FBI") has a system, with the poorly chosen title of "Carnivore," which allows it to examine private e-mails.[8]

---

[7] *See* McVeigh v. Cohen, 983 F. Supp. 215, 217 (D.D.C. 1998) (describing a case of an officer who was discharged on the basis of the gays-in-the-military policy after the government obtained his America Online e-mail and profile where he revealed his homosexuality).

[8] *See infra* note 187 (discussing exaggerated fears of Carnivore); *see also* Ted Bridis, *FBI Won't Provide Data on Carnivore Congress Requested*, WALL ST. J., Aug. 10, 2000, at B8 (discussing the FBI's refusal to disclose information about Carnivore to Congress); Neil King, Jr. & Ted Bridis, *FBI's Wiretaps to Scan E-Mail Spark Concern*, WALL ST. J., July 11, 2000, at A3 (describing concerns regarding the FBI's use of Carnivore); David A. Vise, *Carnivore Going to Review U.*, WASH. POST, Aug. 11, 2000, at A23 (reporting on the

Nevertheless, the differences between crimes that take place in cyberspace and those that occur in realspace should not obscure their similarities. For example, if crime in cyberspace is easier to commit due to technical prowess, then the law needs to consider how to treat offline crimes that harness technical ability. Similarly, if acts in cyberspace portend criminal activity in realspace, then this dangerous complementarity can—if sufficiently strong—justify punishing acts in cyberspace (an example might be electronic stalkers who may graduate to stalking in realspace). This notion undoes the standard idea that criminal punishment should be reserved only for acts that are harmful; the point here is not that a certain act is itself harmful, but that its commission will lead to a harmful act. Preventing the former act is a mechanism the government may use to discourage the commission of the latter.

The problem of cybercrime is really a larger one of how the law deals with new technologies. Sometimes the law treats crimes that employ new technologies as different and deserving of special regulation (such as wire fraud, hijacking of airplanes, and grand theft auto) and at other times it does not (crimes performed with typewriters and most thefts, which carry the same penalty whether accomplished with James Bond-style panache or by a simple break-in). Lurking underneath this differential regulation is a complex symbiotic relationship between technology and law.[9] Computer crime forces us to confront the role and limitations of criminal law, just as criminal law forces us to reconceptualize the role and limitations of technology.

After all, computer crime is not simply constrained by law.[10] Before Bob Ellickson's and Larry Lessig's pathbreaking work, many scholars assumed that law was the primary mechanism for the regulation of conduct. Ellickson and Lessig helped introduce a second constraint, social norms. They showed how such norms can regulate as effectively as law, or even more so.[11] Lessig's recent work

---

Justice Department's plan to review Carnivore by means of a university study).

[9] *See* CAROLYN MARVIN, WHEN OLD TECHNOLOGIES WERE NEW: THINKING ABOUT ELECTRIC COMMUNICATION IN THE LATE NINETEENTH CENTURY 6, 88-97 (1988) (suggesting that electricity and telephones modified crime control).

[10] *See* Neal Kumar Katyal, *Deterrence's Difficulty*, 95 MICH. L. REV. 2385, 2416-20, 2447-55 (1997) (distinguishing among three forms of social regulation: legal sanctions, monetary price, and social norms).

[11] *See generally* ROBERT C. ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES (1991); Lawrence Lessig, *The Regulation of Social Meaning*, 62 U. CHI. L. REV. 943 (1995).

has suggested a third form of regulation, system architecture, or code.[12] Rather than relying on social pressure or legal sanctions, Lessig explains how physical and electronic barriers can prevent harmful acts. In realspace, installing lights on street corners can prevent muggings and other forms of street crime, and placing concrete barricades near inner-city highway ramps can prevent suburbanites from quickly driving in and out to purchase drugs.[13] In cyberspace, internet browsers can be configured to prevent repeated password entry attempts for sensitive web sites or could be coded to prevent certain forms of encryption.

This Article suggests the presence of two other constraints, physical harm and monetary cost. The risk of physical harm in committing a crime is a rather obvious constraint, and one that is lower with computer crime as compared to realspace crime. Monetary costs, by contrast, are not generally thought of by criminal scholars as a deterrent, and this omission is unfortunate. One reason that computer crime is so dangerous is because it is so cheap to perpetrate.

The legal system, I contend, should focus more on perpetration costs. After all, unlike the probabilistic specter of legal sanction, these costs are certain to be incurred by all who commit a crime. In some ways, the legal system's current focus on legal sanctions at the expense of monetary costs is ironic. Criminals tend to be gamblers—willing to speculate on the chance that they will not be caught—and yet the conventional wisdom is to set up a parlor from which to conduct the wager instead of relying on fixed costs that elude speculation and games of chance. Governments use the threat of jail time to deter offenses even though they know that the bulk of offenders discount the threat of long jail sentences because they have many years to live due to their youth. The lack of high perpetration costs is one factor that explains the rise in cybercrime. Indeed, the fact that some forms of crime are cheap to commit weakens the power of social norms; the ease of, for example, copying a CD leads many to think of it as an innocent act.

Monetary costs, in short, may deter a different stratum of the

---

[12] LESSIG, *supra* note 4, at 6.

[13] *See* Fred Musante, *Drug Trade Links Bridgeport and Its Suburbs*, N.Y. TIMES, Feb. 14, 1993, § 13, at 1 ("[T]he police department hopes to discourage the drug buyers by placing concrete highway barriers . . . across dozens of intersections . . . that would make it more difficult for outsiders to get in and out so easily."); Richard Weizel, *A Tentative Farewell to the Bridgeport Barriers*, N.Y. TIMES, July 5, 1998, § 14, at 1.

population than law enforcement—those with less money. Suppose, for example, that the majority of hackers are teenagers. Teenagers, with their lower levels of disposable income, might be particularly responsive to strategies that increase the monetary costs of crime. If dangerous software programs such as hackers' tools were more expensive, or if sensitive web sites charged low admission fees, these forms of regulation may deter criminal wrongdoing in a way that conventional law enforcement may not.[14] This strategy also suggests that when sites such as Napster begin to charge fees for their use, those fees might deter more crime than the speculative risk of a legal sanction. Civil forfeiture of computers and equipment and postconviction restrictions on computer use may also increase perpetration costs and thereby prevent recidivism. Criminal law scholars should incorporate monetary costs into their calculations about optimal deterrence, just as they should recognize social norms and architecture. This multifaceted strategy of regulation is particularly important for those crimes whose offenders tend to be heterogeneous.

Put a different way, the emergence of computer crime threatens an implicit calculus that thus far has constrained realspace crime. Computers make it easier for criminals to evade the constraints of social norms (through pseudonymity and removal from the physical site of the crime), legal sanctions (the probability of getting caught may be reduced for similar reasons), and monetary costs (because the resource inputs necessary to cause a given unit of harm are much lower). The standard Beckerian solution to this problem is to increase the legal sanction, but situating cybercrime within these other constraints reveals other solutions. These other strategies might be more effective because it may be difficult to increase the sanction enough to compensate for a very low probability of getting caught.

Some examples of perpetration cost strategies have been given, so the point will be illustrated by final examples of architectural regulation. Government could redress the lowered constraints against crime by enacting regulations that would prevent pseudonymity by any of the following: (1) by regulating the Internet Protocol ("IP") and software manufacturers (increasing the power of social norms as a constraint on crime, as well as increasing the probability of getting caught); (2) by insisting upon mechanisms that ensure electronic

---

[14] For more about the perverse incentive problem created by such regulation, as well as a fuller discussion of the role of monetary costs in deterrence, see *infra* text accompanying notes 101-07.

tracing of computer signals to locate offenders (increasing the probability of getting caught); or (3) by requiring targets to use software-hardening measures to prevent hackers from interfering with web sites (increasing the perpetration cost of committing these computer crimes). Reasonable people can disagree about the wisdom of each of these solutions; my point is only that because the emergence of computers can reduce all five constraints to crime, our legal solution cannot be blind to these other constraints and focus willy-nilly on the legal sanction.

It is possible, indeed likely, that our blindness to these other constraints is related to the phenomenon discussed earlier, the subtle existence of second and third parties in crime control. After all, it is difficult for the government to increase the monetary cost of crime directly, and it is likewise difficult for government to modify architecture. It can do so at times by fiat, but government shies away from doing so because it is not situated to know which devices are optimal in preventing crime at the cheapest cost. Mistakes made by the government, by mandating the wrong device or strategy, can impose huge deadweight losses. This Article is designed to show how government, by modifying prosecution incentives and altering civil liability and payment rules, can promote cost deterrence and architectural solutions by harnessing second and third parties. These parties enable government to do indirectly what it often has trouble doing directly—change the perpetration cost of crime and modify architecture in ways that prevent criminal acts.

At this stage, an important caveat is in order: this Article is a general treatment of an immensely complicated subject matter. A single article cannot attempt to answer all of the difficult questions about cybercrime strategy. Sometimes it will only pose questions, and other times it will only suggest possible frameworks for approaching problems. This means that some subjects will be considered more comprehensively than others, but selectivity is inevitable given the newness of the field.

One practical consequence of this focus is that this Article must make the simplifying assumption that a central purpose of the criminal law is to deter crime. The Article places deontological concepts to one side and concentrates on ways to make law operate more efficiently in preventing crime. Under other theories of punishment, different conclusions may follow. The purpose of this initial Article is to focus on ways to deter cybercrime with reference to the legal and nonlegal constraints on crime: harnessing first-party

strategies (preventing offenders from committing acts by raising perpetration costs and legal risks), second-party strategies (encouraging victims to protect against attacks, thereby making it more expensive for criminals to commit crimes and easier for them to get caught), and third-party strategies (relying on ISPs and other entities to monitor risky activity and forestall attacks through architectural solutions). My future work will examine the threats posed by law enforcement on the net.[15]

This Article begins by analyzing the various types of crime that can occur online. Virtually every aspect of human interaction—from bank accounts to personal privacy, from the safety of women to the security of our nation's military—is at risk. The Article then explores optimal ways of preventing cybercrime. Moving beyond the conventional strategy of increasing sanctions, the Article explores other constraints on crime. Deterrence may be enhanced by manipulating these other constraints because individuals may lack information about sanctions or probabilities of detection or because they may not be responsive to expected sanctions. At stake here is a theory of deterrence that is focused not only on a criminal's attitudes and knowledge about the law. Instead, law can harness other constraints like monetary price to deter even those who ignore law.

I. WHAT IS CYBERCRIME?

The term "cybercrime" refers to the use of a computer to facilitate or carry out a criminal offense. This can occur in three different ways. First, a computer can be electronically attacked. We may further subdivide this category by distinguishing among acts that involve (1) unauthorized *access* to computer files and programs, (2) unauthorized *disruption* of those files and programs, and (3) *theft* of an electronic identity. An example of the first category is a break-in to Defense Department Computers. An example of the second category is the ILoveYou Worm. The third category, identity theft, occurs when a person's or entity's identity is wrongfully appropriated. A web page may be "page-jacked," for example, so that when you click onto a financial service to read investment news, you receive spurious information instead.[16]

The above crimes involve situations in which a computer is the

---

[15] *See* Neal Kumar Katyal, Law Enforcement on the Net (unpublished manuscript, on file with author).

[16] *See infra* note 68 (discussing the page-jacking of the Bloomberg News Service).

subject of an attack. A rather different type of computer crime occurs when a computer is used to facilitate or carry out a traditional offense.[17] For example, a computer might be used to distribute child pornography over the internet or it might be used to create a massive number of copies of a popular and copyrighted song. Complicated insurance fraud, large check-kiting operations, and other sophisticated forms of white collar crime rely on computers to run the criminal operation.[18] In these cases, computers make it easier to carry out a crime in realspace. In these circumstances, computers are tools that expedite traditional offenses.[19]

As news reports suggest, cybercrime is becoming an increasingly common form of criminal activity. The numbers are staggering. The number of recorded computer security incidents grew from 6 in 1988 to more than 8000 in 1999.[20] Theft on the internet caused $2 billion in losses in the year 1995, a number that is much higher today.[21] One

---

[17] Scott Charney & Kent Alexander, *Computer Crime*, 45 EMORY L.J. 931, 934 (1996).

[18] DONN B. PARKER, FIGHTING COMPUTER CRIME 98-100 (1983). Because of the broad nature of crimes in cyberspace and the ease of committing them, there is no one "type" of cybercriminal. Their profiles span the gamut of society. *See* Mark D. Rasch, *Criminal Law and the Internet*, *in* THE INTERNET AND BUSINESS: A LAWYER'S GUIDE TO THE EMERGING LEGAL ISSUES 141, 142 (Joseph F. Ruh, Jr. ed., 1996) ("[C]omputer criminals are not of a discrete type. They range from the computer world equivalent of a juvenile delinquent, the hacker or cyberpunk, to the sophisticated white-collar embezzler attacking financial institution computers, and include cyberterrorists, extortionists, spies, petty thieves and joyriders.").

[19] Of course, sometimes an act will overlap categories. A boy who breaks into a record label's stored computer recordings to listen to an unreleased song by his favorite band, and who then decides to use Napster to distribute the song to his friends, both commits unauthorized access and carries out a traditional offense. The only important definitional principle at stake is to avoid unnecessarily forcing expansion of the last category, traditional offenses. In today's society, virtually everything has some nexus to a computer. Using WordPerfect to type a threat to the President is rather different than using a computer program to place thousands of copies of copyrighted material on the internet. Rasch, *supra* note 18, at 142-44. In the latter, the computer is achieving something that would be quite difficult to do without computers—namely, rampant distribution of the illegal material. It is this use of hardware and software that this Article addresses.

[20] *Internet Denial of Service Attacks and the Federal Response: Joint Hearing Before the Crime Subcomm. of the House Judiciary Comm. and the Criminal Justice Oversight Subcomm. of the S. Judiciary Comm.*, 106th Cong. (2000) (statement of Sen. Patrick Leahy), 2000 WL 232395 [hereinafter *Cyberattack*, Leahy].

[21] Mark J. Biros & Thomas F. Urban, II, *New Computer Crime Statutes Close Loopholes*, NAT'L L.J., Mar. 25, 1996, at C3. A Computer Security Institute survey reports that 62% of companies have experienced computer break-ins, 51% reported financial losses due to computer security problems, and 27% reported financial fraud. *Cybercrime: Hearing Before the Subcomm. on Commerce, Justice, and State, the Judiciary, and*

company has found 100,000 instances of illegal activity on web sites in one and a half years.[22] New viruses are being launched at the rate of ten to fifteen per day and over 2400 currently exist.[23] Last year, there were more than 22,000 confirmed attacks against Department of Defense computers.[24] It is no surprise that the FBI's caseload has skyrocketed as a result of these trends.[25]

Yet many believe that cybercrime is still in its infancy, and that criminals have not yet reached their potential.[26] It could be said, akin to early 1990s high technology companies, that criminals still lack an adequate "business model" to achieve profit. This is likely to change. As more targets in realspace are hardened against criminal acts, more

---

Related Agencies of the S. Appropriations Comm., 106th Cong. 74 (2000) [hereinafter *Cybercrime Hearing*] (statement of Mark Rasch, Vice President, Global Integrity Corporation). Theft of information and intellectual property has increased 15% from 1998 to the beginning of 2000. *Id.* Unauthorized access by an insider has increased 28% during that time and system penetration by external parties has increased 32%. *Id.*; *see also* Burleson v. State, 802 S.W.2d 429, 433 (Tex. Ct. App. 1991) (affirming the conviction of an employee for using a logic bomb to erase payroll data after he was fired); *Cybercrime Hearing*, *supra*, at 17 (statement of Louis J. Freeh, Director, Federal Bureau of Investigation) (stating that a 1999 Computer Security Institute/FBI survey found that 55% of respondents reported malicious computer activity by corporate insiders—disgruntled employees, computer technicians, and the like); Quentin Hardy, *Firms Are Hurt by Break-Ins at Computers*, WALL ST. J., Nov. 21, 1996, at B4 (reporting that of 205 large American companies, half had their computers penetrated in the past year and 84% of these companies assessed their damage at more than $50,000 per incident).

[22] Bobbi Nodell, *Online Thieves Collide with the Law: A Look at How Copyright Theft Is Being Handled in the Courts* (July 23, 1998), *at* http://www.msnbc.com/news/178744.asp.

[23] *Cyber Threats and the U.S. Economy: Hearing Before the J. Econ. Comm.*, 106th Cong. (2000) (statement of Vinton Cerf, Senior Vice President, MCI Worldcom), 2000 WL 11068387 [hereinafter *Cyberthreats*, Cerf]. More than four million computer hosts were affected by computer security incidents involving viruses in 1999 alone. *Cyberattack*, Leahy, *supra* note 20.

[24] Mathew Schwartz, *For Hire: Hackers to Help Pentagon Prevent Attacks*, (Aug. 1, 2000), *at* http://www.cnn.com/2000/TECH/computing/08/01/pentagon.at.defcon.idg/index.html.

[25] *See Internet Denial of Service Attacks and the Federal Response: Joint Hearing Before the Crime Subcomm. of the House Judiciary Comm. and the Criminal Justice Oversight Subcomm. of the S. Judiciary Comm.*, 106th Cong. (2000) (statement of Michael A. Vatis, Director, FBI National Infrastructure Protection Center), 2000 WL 234743 [hereinafter *Cyberattack*, Vatis] (describing an "exponential[]" increase in caseload and stating that cases have increased from 206 in 1997 to over 900 today); *Cybercrime Hearing*, *supra* note 21, at 23 (statement of Louis J. Freeh, Director, Federal Bureau of Investigation) (same).

[26] *See Cyber Threats and the U.S. Economy: Hearing Before the J. Econ. Comm.*, 106th Cong. (2000) (statement of Dr. Mark Graff, Sun Microsystems), 2000 WL 11068388 [hereinafter *Cyberthreats*, Graff] (pointing to the present lack of "sufficient economic or martial incentive" as the reason for so few "substantial attacks against" the internet).

geographic substitution from realspace to cyberspace will occur.[27] As early as ten years ago, reports began to describe computer crime as the "weapon of choice" among white-collar criminals.[28]

Nevertheless, law enforcement has not responded adequately to the threat. As one industry analyst put it, "law enforcement online ranges from haphazard to nearly nonexistent."[29] Erasure programs destroy electronic footprints, making tracking very difficult and facilitating a cybercriminal's escape.[30] Although enforcement is weak, federal law against cybercrime has been expanded. The current federal computer crimes statute, 18 U.S.C. § 1030, prohibits certain forms of unauthorized access (and prohibits exceeding authorized access) to any "protected computer."[31] "Protected computers," in turn, include virtually every computer connected to the internet, for the law protects any computer used across state lines.[32] Section 1030 prohibits access to a computer when access is used to obtain national security information or financial records, intercept interstate communications, manipulate government computers, defraud and obtain anything worth $5000 or more, traffic in passwords, or extort by threatening to damage a protected computer.[33] The statute carries

---

[27] *See* Katyal, *supra* note 10, at 2421 (describing geographic substitution as a phenomenon occurring when crime moves away from a high-enforcement area to a low-enforcement one).

[28] Ray Quintanilla, *Computer Crimes Newest Nemesis for Regulators, Police Departments*, INVESTOR'S DAILY, Mar. 9, 1990, at 25.

[29] *Cybercrime Hearing*, *supra* note 21, at 63 (statement of Jeff B. Richards, Executive Director, Internet Alliance); *see also* Marc D. Goodman, *Why the Police Don't Care About Computer Crime*, 10 HARV. J.L. & TECH. 465, 477-78 (1997); Paul Korzseniowski, *Computers Made Plain—More Hackers, Viruses Have the FBI Leading Attack for Security Funding*, INVESTOR'S BUS. DAILY, July 21, 2000, at A4 (quoting an industry analyst as stating that "'[c]omputer technology has been evolving so rapidly that government enforcement agencies have not had the resources needed to keep pace'"). According to one leading DOJ Computer Crime prosecutor, "[t]he chances of detection and prosecution of computer hackers is very small." *Cybercrime Hearing*, *supra* note 21, at 80 (statement of Mark Rasch, Vice President, Global Integrity Corporation).

[30] *See Cybercrime Hearing*, *supra* note 21, at 73 (statement of Mark Rasch, Vice President, Global Integrity Corporation) (stating that computer hackers are becoming increasingly sophisticated and creative, and therefore more difficult to detect and prosecute); *see also infra* text accompanying note 183 (discussing the additional difficulties of tracing electronic footprints when criminals use pseudonymous e-mail addresses or weave their footprints through a series of computers).

[31] 18 U.S.C. § 1030 (Supp. IV 1998).

[32] *Id.* § 1030(e)(2)(B).

[33] *Id.* § 1030(a)(1)-(7). In 1994, Congress modified § 1030 to state that the requisite mens rea was "intentional, knowing, and reckless," but that amendment was further modified in 1996 to impose strict liability. *See* S. REP. NO. 104-357, at 10-11 (revealing that Congress wanted to punish hackers who do not intentionally cause

a mandatory-minimum sentence of six months.[34]

The federal computer crimes statute is only the beginning of government regulation. Criminal law scholars have not noticed that when Vermont enacted a statute proscribing computer crime in 1999, it became the fiftieth state to devote specific legislation to computer crimes. The two activities that most states criminalize are (1) unauthorized access to a computer with intent to do some further bad act and (2) damage to computer-related property (including intangible property).[35] Put briefly, "unauthorized access with intent"

---

damage to computers but nevertheless commit "computer trespass"); *see also* United States v. Sablan, 92 F.3d 865, 868 (9th Cir. 1996) (holding that the computer fraud statute does not require proof that the defendant had an intention to damage computer files); Haeji Hong, Note, *Hacking Through the Computer Fraud and Abuse Act*, 31 U.C. DAVIS L. REV. 283, 284 (1997) (documenting changes made to the mens rea requirement in § 1030).

[34] Perversely, § 1030's mandatory-minimum sentence has created an inverse sentencing effect whereby prosecutors do not prosecute computer crime cases because of the draconian minimum sentence. *See* Letter from Charles E. Schumer, United States Senator, to Colleagues (Feb. 16, 2000) ("As a result [of the minimum sentence], some prosecutors have declined to bring cases, knowing that the result would be mandatory imprisonment."), *available at* http://www.cdt.org/policy/terrorism/000216schumer.shtml.

[35] States use different and sometimes conflicting terminology in classifying computer crimes. I am attempting to generalize the types of acts proscribed by these statutes rather than simply adopting the names of the crimes (especially because the same name is occasionally used by different states to capture different acts). The statutes analyzed are ALA. CODE §§ 13A-8-100 to -103 (1994); ALASKA STAT. §§ 11.46.200(a)(3), 11.46.484(a)(5), 11.46.740, 11.46.985 (Lexis 2000); ARIZ. REV. STAT. ANN. §§ 13-2301(E), 13-2316 (West 1989 & Supp. 2000); ARK. CODE ANN. §§ 5-41-101 to -108 (Michie 1997); CAL. PENAL CODE §§ 502, 502.01, 1203.047 (West 1999 & Supp. 2001); COLO. REV. STAT. §§ 18-5.5-101 to -102 (1986 & Supp. 1996); CONN. GEN. STAT. ANN. §§ 53a-250 to -261 (West 1994 & Supp. 2000); DEL. CODE ANN. tit. 11, §§ 931-939 (1999 & Supp. 2000); FLA. STAT. ANN. §§ 815.01 -.07 (West 2000); GA. CODE ANN. §§ 16-9-90 to -94 (Lexis 1999); HAW. REV. STAT. §§ 708-890 to -893 (1993); IDAHO CODE §§ 18-2201 to -2202, 26-1220 (Michie 1997); 720 ILL. COMP. STAT. ANN. 5/16D-1 to -7 (West 1993 & Supp. 2000); IND. CODE ANN. §§ 35-43-1-4, 35-43-2-3 (West 1998); IOWA CODE ANN. §§ 716A.1-.16 (West 1993 & Supp. 2000); KAN. STAT. ANN. § 21-3755 (1995 & Supp. 2000); KY. REV. STAT. ANN. §§ 434.840-.860 (Michie 1999); LA. REV. STAT. ANN. §§ 14:73.1-.5 (West 1997 & Supp. 2001); ME. REV. STAT. ANN. tit. 17-A, §§ 431-433 (West Supp. 2000); MD. ANN. CODE art. 27, § 146 (1996 & Supp. 2000); MASS. ANN. LAWS ch. 266, §§ 30, 33A, 120F (Law. Co-op. 1992 & Supp. 2000); MICH. COMP. LAWS ANN. §§ 752.791-.797 (West 1991 & Supp. 2000); MINN. STAT. ANN. §§ 609.87-.891 (West 1987 & Supp. 2001); MISS. CODE ANN. §§ 97-45-1 to -13 (1999); MO. ANN. STAT. §§ 569.093-.099 (West 1999); MONT. CODE ANN. §§ 45-6-310 to -311 (1999); NEB. REV. STAT. §§ 28-1343 to -1348 (1998); NEV. REV. STAT. ANN. §§ 205.473-.513 (Michie 1997 & Supp. 1999); N.H. REV. STAT. ANN. §§ 638:16 to :34 (1995); N.J. STAT. ANN. §§ 2A:38A-1 to -6, 2C:20-23 to -34 (West 1995 & Supp. 2000); N.M. STAT. ANN. §§ 30-45-1 to -7 (Michie 2000); N.Y. PENAL LAW §§ 156.00-.50 (McKinney 1999); N.C. GEN. STAT. §§ 14-453 to -458 (1999); N.D. CENT. CODE § 12.1-06.1-08 (1997);

criminalizes using a computer outside the scope of one's authority when one has malevolent intent. One need not actually accomplish what was intended, although success in the criminal enterprise would usually affect the penalty imposed.[36] Also, depending on the state, the person need not actually do anything after he has exceeded lawful access.[37] As long as the malevolent intent exists, a person commits this crime the moment he exceeds his lawful access.[38] "Damage to computer-related property" is more straightforward. The crime has been committed when a person damages a computer, computer systems, computer data, computer programs, or other computer-related property.

The patchwork of state laws reveals other patterns in criminalizing certain computer-related activities. Many states designate the theft, interruption, or denial of computer services as an independent

---

OHIO REV. CODE ANN. § 2913.04(D) (Anderson 1996); OKLA. STAT. ANN. tit. 21, §§ 1951-1958 (West Supp. 2001); OR. REV. STAT. §§ 164.125, 164.377 (1990 & Supp. 1998); 18 PA. CONS. STAT. ANN. § 3933 (West Supp. 2000); R.I. GEN. LAWS §§ 11-52-1 to -8 (1997 & Supp. 1999); S.C. CODE ANN. §§ 16-16-10 to -40 (Law. Co-op. 1985 & Supp. 2000); S.D. CODIFIED LAWS §§ 43-43B-1 to -8 (Michie 1997); TENN. CODE ANN. §§ 39-14-601 to -603 (1997); TEX. PENAL CODE ANN. §§ 33.01-.04 (Vernon & Supp. 2001); UTAH CODE ANN. §§ 76-6-701 to -705 (1999); VT. STAT. ANN. tit. 13, §§ 4101-4107 (Supp. 2000); VA. CODE ANN. §§ 18.2-152.2 to .14 (Michie 1996 & Supp. 2000); WASH. REV. CODE ANN. §§ 9A.52.110-.130 (West 2000); W. VA. CODE ANN. §§ 61-3C-1 to -21 (Lexis 2000); WIS. STAT. ANN. § 943.70 (West 1996); WYO. STAT. ANN. §§ 6-3-501 to -505 (Lexis 1999).

[36] For example, Alabama technically criminalizes only unauthorized access, but the punishment for the crime (normally a Class A misdemeanor) is increased to a Class C felony if the offense was committed, among other things, "for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property." ALA. CODE §§ 13A-8-102(d)(1)-(2) (1994).

[37] Some states, such as California, specifically punish particular bad uses of data obtained after an intruder secures access. *See* CAL. PENAL CODE § 502(c)(1) (West Supp. 2001) (criminalizing one who "[k]nowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data").

Other states also criminalize the unauthorized access of a computer, even if no malevolent intent exists. *See, e.g.*, ALASKA STAT. § 11.46.200(a)(3) (Lexis 2000) (specifying a reckless disregard standard for theft of computer services); KAN. STAT. ANN. § 21-3755(d) (2000) ("Computer trespass is intentionally, and without authorization accessing or attempting to access any computer . . . .").

[38] The list of "bad acts" from which a prosecutor chooses what the cybercriminal "intended" varies by jurisdiction. However, common "bad acts" include "[d]evising or executing any scheme or artifice to defraud or extort," ARK. CODE ANN. § 5-41-103(a)(1) (Michie 1997), and "wrongfully control[ling] or obtain[ing] money, property, or data," CAL. PENAL CODE § 502(c)(1)(B) (West Supp. 2001).

crime.[39] Some state statutes explicitly criminalize the introduction of computer viruses and other bugs.[40] Some states criminalize the disclosure of passwords or other computer security information.[41] A few statutes include e-mail crimes, typically punishing either harassing or unsolicited bulk e-mail.[42] However, the difficulty in finding cybercriminals, combined with the difficulty of enforcing state laws across various jurisdictions, makes state prosecution almost impossible.[43]

Not only are federal and state government measures to prevent cybercrime generally lacking, private industry has not kept up to the task of securing its own data either. "Most have no system manager [and] one person may handle dozens or hundreds of systems. [It is h]ard enough to keep the software current and users happy, let alone

---

[39] Connecticut's theft provision is representative: "A person is guilty of the computer crime of theft of computer services when he accesses or causes to be accessed or otherwise uses or causes to be used a computer system with the intent to obtain unauthorized computer services." CONN. GEN. STAT. ANN. § 53a-251(c) (West Supp. 2000). Delaware provides a good example of an interruption/denial provision: "A person is guilty of the computer crime of interruption of computer services when that person, without authorization, intentionally or recklessly disrupts or degrades or causes the disruption or degradation of computer services or denies or causes the denial of computer services to an authorized user or a computer system." DEL. CODE. ANN. tit. 11, § 934 (1999).

[40] Maine's provision is a good example; a person is a criminal if he "[i]ntentionally or knowingly introduces or allows the introduction of a computer virus into any computer resource, having no reasonable ground to believe that the person has the right to do so." ME. REV. STAT. ANN. tit. 17-A, § 433(1)(C) (West Supp. 2000).

[41] *E.g.*, 18 PA. CONS. STAT. ANN. § 3933(a)(3) (West Supp. 2000).

[42] For example, Arkansas sanctions a person when, "[w]ith the purpose to frighten, intimidate, threaten, abuse, or harass another person, he sends a message to the person on an electronic mail or other computerized communications system and in that message threatens to cause physical injury" or property damage or uses any obscene, lewd, or profane language. *See* ARK. CODE ANN. § 5-41-108(a)(1) (Michie 1997). The constitutionality of at least a portion of this provision is certainly questionable. The other tactic used by states is to criminalize the sending of unsolicited bulk e-mail when the sender has forged his identity. For instance, Illinois sanctions a person who "[f]alsifies or forges electronic mail transmission information or other routing information in any manner in connection with the transmission of unsolicited bulk electronic mail through or into the computer network of an electronic mail provider or its subscribers." 720 ILL. COMP. STAT. ANN. 5/16D-3(5) (West 2000).

[43] *See* DOJ REPORT, *supra* note 5, at 34 (noting serious barriers to state prosecution, including lack of resources, long-arm jurisdiction, electronic surveillance, and subpoena power); *Cybercrime Hearing*, *supra* note 21, at 30 (statement of Louis J. Freeh, Director, Federal Bureau of Investigation) (explaining that state investigators often lack the training necessary in cybercrime cases).

watch for intruders breaking in or grabbing passwords."[44] While the average computer has become more secure, the sheer explosion in the number of computers—and society's reliance on them—has meant that our overall security has dropped precipitously. In part, this is because many crimes go undetected and unreported.[45]

Due to the ever-increasing amounts of jargon, a brief description of some of the major forms of cybercrime may help facilitate the theoretical discussion. My aim, again, is not to set out iron-clad categories as much as it is to describe some of these crimes before moving to the heart of the paper.[46]

---

[44] CLIFFORD STOLL, SILICON SNAKE OIL 107 (1995).

[45] One government study deliberately attacked 38,000 government computers and successfully penetrated 65% of them. Systems administrators detected only 4% of those penetrations. Of the 4%, only 27% of them were reported. In other words, there were only 267 reports by administrators arising from the successful penetration of the 24,700 machines—about 1 report per 100 violations. Charney & Alexander, *supra* note 17, at 936; *see also* U.S. GEN. ACCOUNTING OFFICE, INFORMATION SECURITY: COMPUTER ATTACKS AT DEPARTMENT OF DEFENSE POSE INCREASING RISKS 2-3 (1996) (summarizing defense risks from outside attacks). As the Former Director of the FBI Computer Crime Squad put it, "You bring me a select group of 10 hackers and within 90 days, I'll bring this country to its knees." Chris O'Malley, *Information Warriors of the 609th*, POPULAR SCI., July 1997, at 71, 72.

Another reason computer attacks are so easy is that computer operating systems and other major software packages are still riddled with security flaws. Computer crime can be prevented either with better government prosecution or with better private software protection. Code can prevent cybercrime by closing weak areas and bugs that hackers exploit to gain access to data. Yet this has not happened. As one major industry representative puts it, "Looking under the hood of all the major operating systems in use today, we find the same kinds of security flaws, coding errors, and faulty assumptions programmers like myself were turning out in the Seventies and Eighties." *Cyberthreats*, Graff, *supra* note 26.

[46] This Article does not directly focus on analogues to realspace crime that create a harm solely or predominantly in cyberspace. For example, it will not directly deal with the perplexing matter of whether one's computer identity can be harmed. The most common example here is "virtual rape" of a person on the internet. *See* LESSIG, *supra* note 4, at 75; Julian Dibbell, *A Rape in Cyberspace or How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database into a Society*, 1994 ANN. SURV. AM. L. 471 (providing a detailed account of the "virtual rape" that occurred in Lambda Moo, a chat room). Such acts, while in no way similar to their realspace counterparts, can have serious consequences in realspace. For example, they may destroy internet communities, and these communities may be essential places for learning, sharing, and the like. Virtual rape, and other such acts, can impose psychological harm. Dibbell, *supra*, at 475-76. These electronic acts may also have complementarity with their realspace counterparts, and the law accordingly might intervene. *See infra* text accompanying notes 87-95.

A. *Unauthorized Access to Computer Programs and Files*

Unauthorized access occurs whenever an actor achieves entry into a target's files or programs without permission. The actor may be a person or another computer, and the access may be achieved electronically (through passwords and other mechanisms) or physically (by, for example, breaking into a file cabinet and stealing a personal identification number ("PIN")). Electronic access is by far the more common threat, and it is perpetrated by those who steal passwords, use computers to generate random passwords until entry is accomplished, or use "trap doors" to enter a secure area.[47] A trap door is a fast way into a computer program that allows program developers to bypass security protocols built into the program. Programmers and software manufacturers place trap doors in programs so that they can quickly modify the underlying code. But these doors also permit anyone with a modest level of computer sophistication to break into a computer and run it in any way he or she sees fit. For example, a ubiquitous computer platform in the late 1980s—UNIX—contained a trap door that allowed anyone to break into mainframe computer systems and run them from a remote location. East German agents penetrated the University of California at Berkeley's computers in one such attack.[48] The crime of unauthorized access is one of simply invading another's workspace. Causing harm to the files or programs or using the data improperly are treated as separate crimes.

There are several different targets for unauthorized access; broadly speaking, they may be categorized as the government, individuals, or commercial entities. The government has vast information on its computers, ranging from nuclear secrets to defense planning contingencies and from human intelligence to law enforcement information about criminal organizations. The specter of a curious computer geek who gains access to sensitive computers—popularized in the 1983 film "War Games"—is not fanciful, as such attacks have occurred successfully on numerous occasions.

---

[47] Passwords are commonly stolen through the use of "sniffer" programs. These programs monitor a user's keystrokes, and transmit the information back to the host computer that initiated the sniffer program. The electronic thief then has a full transcript of the passwords necessary to achieve entry into a system. In 1994 as many as 100,000 sites were affected by sniffer attacks. DAVID ICOVE ET AL., COMPUTER CRIME: A CRIMEFIGHTER'S HANDBOOK 51 (1995).

[48] *See generally* CLIFFORD STOLL, THE CUCKOO'S EGG: TRACKING A SPY THROUGH THE MAZE OF COMPUTER ESPIONAGE (1989).

Unauthorized access to such material can pose severe security risks. By contrast, unauthorized access to an individual's personal files presents a different set of harms. These harms are generally harms to privacy, as personal files contain private and intimate thoughts. These thoughts may be as personal as love letters, as banal as grocery lists, or as tragic as unfinished drafts of law review articles. In any event, the computer thief gains access to that information without permission. Commercial access, by contrast, may place at risk a company's proprietary information and trade secrets. There also may be individual privacy interests at stake (such as personnel files), but the interests here will largely be financial ones.

The different types of targets suggest that different motivations may be at stake for each type of crime: to gain financial benefits (copyright theft, trade secrets),[49] to benefit a foreign enemy (espionage),[50] to gain personal satisfaction (spying on a boyfriend or enemy), to thwart law enforcement (by obtaining identities of informants),[51] or to exact revenge (a fired employee who wreaks computer havoc).[52] Additional targets may include hospitals and

---

[49] For example, a group dubbed "the phonemasters" broke into MCI and AT&T computers to steal thousands of calling card numbers and then sold the numbers. The numbers eventually wound up in the hands of Italian organized crime groups. *Cybercrime Hearing*, *supra* note 21, at 17-18 (statement of Louis J. Freeh, Director, Federal Bureau of Investigations).

[50] Chinese military thinking considers computer network attacks an important means for waging warfare. *Cyber Threats and the U.S. Economy: Hearing Before the J. Econ. Comm.*, 106th Cong. (2000) (statement of Dr. Daniel T. Kuehl, National Defense University), http://www.ndu.edu/irmc/publications/congress2.htm [hereinafter *Cyberthreats*, Kuehl]. The *Journal of Slavic Military Studies* reveals that Russia has also been developing an information warfare capacity. One Russian theorist suggested that the potential "psychological impact on the United States would be huge if the financial markets go down" due to cybercrime. *Id.*

[51] The Mafia families need computer capabilities for three reasons. First, they engage in large scale business, whether operating a bank in Los Angeles or running drugs in Florida. Therefore, like any large business, they need the computers available to them through their legitimate business holdings. Second, they need computer technology capabilities to engage in crime against organizations that use computers. Third, national and state or regional governments use computers in their organized crime investigation and prosecution functions. Therefore, crime organizations need a technical capability to attack those powerful tools, which can be so effective in tracking them and their activities.

PARKER, *supra* note 18, at 108-09; *see* Joshua C. Ramo, *Crime Online: Mobsters Around the World are Wiring for the Future. Can the Cops Keep Up?*, TIME, Sept. 23, 1996, at 32 (stating that the Italian Mafia, Chinese gangs, Russian organized crime, and Colombian cartels are employing computer hackers).

[52] ICOVE ET AL., *supra* note 47, at 118.

research institutions with important data.[53]

If a criminal uses the fruits of an unauthorized access, the results may be devastating. Military secrets could be turned over to terrorist rogue states; people's most private thoughts could be placed on the internet for all to see; a company's most cherished secrets—the formula for Coca-Cola and the like—could be given to rival firms;[54] and assets may be shaved off for profit. Although these are four separate types of activity, each shares the common nucleus of unauthorized access combined with distribution of the information to others.

B. *Unauthorized Disruption*

Unauthorized disruption is the heart of what most people consider cybercrime. It occurs when an entity, without permission, interferes with the functionality of computer software or hardware. By now, the lingo is familiar—viruses, worms, logic bombs, Trojan horses, and denial-of-service attacks.

1. Viruses

A virus is a program that modifies other computer programs. The modifications ensure that the infected program replicates the virus. In other words, the original program (the analogue to a healthy cell) is changed by the virus so that the virus can multiply. Once infected, the program secretly requests the computer's operating system to add a copy of the virus code to the target program.[55] Once that computer is connected to another computer, either through the internet, direct computer connection, or even through a common floppy disk, the

---

[53] *See* Laura DiDio, *A Menace to Society*, NETWORK WORLD, Feb. 6, 1989, at 71, 84 (describing how a computer virus attacked a large hospital and destroyed more than forty percent of its patient records); Christopher Elliott, *Experts To Classify Computer Viruses*, SUNDAY TELEGRAPH (London), Mar. 10, 1991, at 2 (noting that an Italian university lost one year of AIDS research data due to a computer virus).

[54] Alternatively, the perpetrators of the theft could blackmail the victim for return of the information. In January 2000, "a group of intruders based in the United Kingdom broke into the computer systems of at least 12 multinational companies and stole confidential files. The group issued ransom demands of up to 10 million [British pounds] in exchange for the return of the files." *Cyber Threats and the U.S. Economy: Hearing Before the J. Econ. Comm.*, 106th Cong. (2000) (statement of Stephen E. Cross, Director, Software Engineering Institute, Carnegie Mellon University), 2000 WL 11068413 [hereinafter *Cyberthreats*, Cross].

[55] Peter J. Denning, *Computer Viruses*, *in* COMPUTERS UNDER ATTACK 285, 286-87 (Peter J. Denning ed., 1990).

virus may spread beyond the original host computer. A virus is not inherently harmful—its harmfulness will depend on the additional codes placed into the virus besides the code for self-replication. Some viruses, however, have caused enormous damage.[56]

2. Worms

A worm is a stand-alone program that replicates itself. Both worms and viruses self-replicate. The distinction is that while a virus requires human action, from downloading a specific file to placing an infected disk in a computer, a worm uses a computer network to duplicate itself and does not require human activity for transmission. The infamous ILoveYou bug shared elements of both viruses and worms. It resembled a virus because it bred on a host computer's hard drive, but was a worm because it reproduced without any additional human input over a network.[57] More than one million

---

[56] A recent example is the Melissa virus, which became famous in March 1999. Melissa infected its first victim when a reader of the pornographic alt.sex newsgroup caught it. Jim Conley, *Germ Warfare*, ZIFF DAVIS SMART BUS. FOR NEW ECON., June 1, 2000, at 62, 65. Within days of this initial contact, Melissa infected more than one hundred Fortune 1000 companies. *Id.* The virus operated by e-mailing a list of eighty pornographic web sites to fifty e-mail addresses in the electronic address book of the infected system. *Id.* The fifty recipients received e-mails with the subject line "Important Message From . . ." and the virus automatically filled in the initial user's name—so that it appeared that the recipient was receiving a message from his or her friend, rather than from the Melissa culprit. Rose Simmons, *Computer Users Fell Hard for the Love Bug*, ASBURY PARK PRESS, May 12, 2000, at 23. The e-mail systems of the fifty recipient computers then were infected, and each passed the virus to fifty additional addresses. *Id.* When this process was repeated over and over, the number of affected computers increased dramatically. As a result, the virus caused many millions of dollars in damage to computers worldwide; in the United States alone, the virus affected 1.2 million computers in one-fifth of the country's largest businesses. *Id.* David Smith pleaded guilty last December to state and federal charges associated with his creation of the Melissa virus. *Id.*; *see also* John Snell, *Think You've Seen Computer Viruses? Hold onto Your Mouse*, STAR TRIBUNE (Minneapolis), Apr. 3, 2000, at 2E ("For all the trouble Smith now finds himself in, there is no shortage of virus writers waiting to follow the trail he blazed.").

[57] The ILoveYou bug was spread primarily through e-mail, but was also transmitted through internet chat and company intranet systems. Here is how most users were infected. First, a user would open an e-mail, entitled "ILOVEYOU," and its attachment, entitled "LOVE-LETTER-FOR-YOU.TXT.vbs." Then the bug installed itself in the computer's system. Once the machine was restarted, the bug spread by mailing itself to everyone in the user's e-mail address book, using the popular Microsoft Outlook Express. The bug then overwrote certain files with extensions such as .jpg, .jpeg, .mp3, and .mp2, deleting them and leaving infected copies of the files in the computer. The bug also used the Internet Explorer home page to download a program that stole passwords and mailed them to e-mail addresses in the Philippines. Finally, the bug changed the default home page to one of the four Web pages hosted

computers in North America alone received a copy of the bug, and it spread nine times faster than the Melissa virus. Most companies, including AT&T Corp., Ford Motor Co., and Merrill Lynch & Co., shut down their e-mail systems to prevent a spread of the attack, resulting in lost time and productivity. Government agencies were also affected, including the Pentagon, the CIA, NASA, the Swiss Government, Danish Parliament, and the British House of Commons. Investigators traced the ILoveYou bug to several computer students in the Philippines, but the case was ultimately dropped because the Philippines had no applicable law against viruses or hacking.[58]

3. Logic Bombs and Trojan Horses

A logic bomb tells a computer to execute a set of instructions at a certain time under certain specified conditions.[59] Those commands could be benign (a nice message from the programmer each year on her birthday) or damaging (telling the hard disk to erase itself on May Day). A logic bomb can lie undetected in software or hardware, ready to be detonated when a series of events unfolds. Sometimes the logic bomb will be used to help facilitate an attack in realspace, such as a bank robber who shuts down bank security through software at 3:00 p.m. on a given Friday. Other times it may be used to demonstrate someone's displeasure with a particular act, such as using Microsoft

---

by skyinet.net, a Philippine Internet Service Provider.

The perpetrators were discovered because one of them, Onel A. de Guzman, had proposed a thesis to a professor exploring the ability to steal computer passwords. The proposal was rejected because of its immorality. This helped link Philippine investigators to de Guzman and another primary suspect, Michael Buen. The duo posted the password-stealing program on the Web using an internet service provider in Manila. That service provider, as well as another provider that Guzman and Buen subsequently hacked into, had caller-identification technology, which allowed technicians to pinpoint the phone number quickly. Foolish mistakes by the suspects led investigators to an apartment owned by de Guzman's sister. A search of the apartment produced little evidence since the original computers and disks had been removed. *See Any Idiot Can Make a Virus*, STRAITS TIMES (Singapore), July 12, 2000; John Schwartz, *No Love for Computer Bugs*, WASH. POST, July 5, 2000, at A1.

[58] *Philippines Drops Charges in "ILoveYou" Virus Case*, *supra* note 2. Another example of a worm was the "Joke" e-mail sent to about 13,000 people in June 2000. This e-mail said it was a joke and when opened, said, "this is funny" or "funny." When the actual attachment, titled "Life-Stages-.txt.shs" was opened, the worm spread much like the ILoveYou bug. Another famous example is the Robert Morris case, in which a Cornell student launched a worm that ultimately caused major computer havoc. *See* Ted Eisenberg et al., *The Cornell Commission: On Morris and the Worm*, *in* COMPUTERS UNDER ATTACK, *supra* note 55, at 253, 254.

[59] MICHELLE SLATALLA & JOSHUA QUITTNER, MASTERS OF DECEPTION 75-76 (1995).

Explorer, or using America Online to trade tobacco stocks.[60] Infecting software code with a logic bomb is a powerful way to magnify a crime so that its effects are far greater than they would be were the crime committed in realspace. The bomb resides in each version of the software, and millions of copies might be sold, all ready to detonate at a certain time. With a logic bomb, instead of just assaulting one computer, an attacker can reach thousands or even millions at once.

A Trojan horse, by contrast, is a computer program that performs some apparently useful function, but which also contains malicious hidden code.[61] The malicious code may introduce a virus or other computer bug or it may permit unauthorized access by an outside user. Indeed, a Trojan horse is the most common way in which viruses are introduced into computer systems.[62] A horse is generally placed in a software program, although it may also be placed in hardware, as was done in Sweden in the early 1980s.

4. Distributed Denial of Service

Distributed Denial of Service ("DDOS") attacks overwhelm web sites and stop them from communicating with other computers. To carry out a DDOS attack, an individual obtains unauthorized access to a computer system and places software code on it that renders that system a "Master." The individual also breaks into other networks to place code that turns those systems into agents (known as "zombies" or "slaves"). Each Master can control multiple agents. In both cases, the network owners become third-party victims, for they are unaware that dangerous tools have been placed on their systems. The Masters are activated either remotely or by internal programming (such as a command to begin an attack at a prescribed time) and are used to send information to the agents. After receiving this information, the agents make repeated requests to connect with the attack's ultimate target, typically using a fictitious or "spoofed" IP address, so that the recipient of the request cannot learn its true source. Acting in unison, the agents generate a high volume of traffic from several sources. This type of attack is referred to as a SYN flood (SYN is the

---

[60] *See, e.g.*, State v. Corcoran, 522 N.W.2d 226 (Wis. Ct. App. 1994) (involving a computer programmer who, to guarantee that he would be paid to write a computer program, inserted code in the program that erased data when the computer's clock reached a specified time, and was subsequently prosecuted under the Wisconsin Computer Crimes Act).

[61] Denning, *supra* note 55, at 286.

[62] *Id.* at 288.

initial effort by the sending computer to make a connection with the destination computer). Due to the volume of SYN requests, the destination computer becomes overwhelmed in its efforts to acknowledge and complete transactions with each sending computer. As a result, it loses all or most of its ability to serve legitimate customers—thus the term Distributed Denial of Service.[63]

In February 2000, a fifteen-year-old Canadian youth known as "MafiaBoy" allegedly used a DDOS attack to shut down popular internet sites such as Yahoo!, Amazon.com, Buy.com, E*Trade, CNN.com, and others. The youth used three computers to flood the target sites, including a computer at the University of California. MafiaBoy's attack revealed to many consumers the vulnerability of internet business, thus contributing to a 258.44-point slide in the Dow Jones Industrial Average and ending a string of record-high closes on the NASDAQ Composite Index. It is typically very difficult to track DDOS hackers because the flood of illegitimate requests comes from remote computers, not the hacker's own computer. Indeed, MafiaBoy set up "dummy" web sites to make the original source of the requests even more difficult to trace. FBI agents only learned of MafiaBoy through his bragging in internet chat rooms about shutting down the world's leading internet sites;[64] had he remained silent, he may never have been caught.

C. *Theft of Identity*

Identity theft occurs when one's identity is wrongfully appropriated by another. Some forms of identity theft via computer are familiar. Joe may pose as Frank on Buy.com and use Frank's credit card to purchase a stereo, or Frank may pose as Joe and send hurtful e-mails to Joe's girlfriend to dissolve Joe's relationship. These situations are computer versions of familiar crimes (credit card theft and forged letters); cyberspace simply makes them easier to commit.

Other types of identity theft via computer, such as cross-site scripting, IP spoofing, and page-jacking, do not have clear realspace analogues. Cross-site scripting occurs when code is placed into a web site to force it to send out information against the will of its owners.

---

[63] *See Cyberattack*, Vatis, *supra* note 25 (commenting that "while attack tools [for DDOS attacks] have become more sophisticated, they have also become easier to use").

[64] *See* Kevin Johnson et al., *Online Boasting Leaves Trail*, USA TODAY, Apr. 20, 2000, at 1A.

With IP spoofing, a perpetrator, using software, impersonates a computer trusted by the victim. As a result, the attacker computer—believed by the victim computer to be a different, friendly computer—achieves entry into sensitive areas or even control of the victim computer by operating privileged protocols.[65] Page-jacking occurs when a link, logo, or other internet address is reprogrammed to bring a customer not to the intended site, but to some other one. For example, if I click on the "Buy.com" logo on the CNN web site, and it brings me not to Buy.com, but rather to an internet gambling web site, the page has been jacked.

D. *Carrying Out a Traditional Offense*

Computers can be used to carry out virtually any offense in realspace, from furthering organized crime to manipulating stocks.[66] Here, I will focus on four exemplars of criminal activity in this category: pornography, copyright piracy, cyberstalking, and the illegal sale of firearms. Each reveals the advantages, from the criminals' perspective, of cybercrime—widespread, quick distribution and cost minimization.

1. Child Pornography

Whereas a piece of child pornography once might have only reached a few thousand people who bought a magazine, with the internet it can reach millions very quickly.[67] The child pornographer in realspace is constrained by all kinds of production costs (film, printing, distribution), but these constraints do not pose the same difficulty to the pornographer in cyberspace. Ease of distribution is a standard feature of cybercrime. Even financial crimes, such as stock market manipulation, take advantage of this feature. For example, someone holding XYZ stock will announce on message boards the

---

[65] *See Cyberthreats*, Cross, *supra* note 54 (describing how "cross-site scripting" can fool web browsers into running malicious code even on trustworthy sites).

[66] An increasing number of illegal drug traffickers . . . are also using the Internet. With portable computers and online connections, illegal drug traffickers can transmit text, audio, and video; track shipments; and engage in financial transactions virtually anywhere in the world. In short, . . . drug traffickers are turning to innovative technologies to conduct their businesses, disguise their activities, and avoid law enforcement scrutiny.

DOJ REPORT, *supra* note 5, at D-2.

[67] LESSIG, *supra* note 4, at 170; Niva Elkin-Koren & Eli M. Salzberger, *Law and Economics in Cyberspace*, 19 INT'L REV. L. & ECON. 553, 556 (1999).

likelihood of a hostile takeover of XYZ, thousands will read the message and purchase XYZ, and the person who posted the messages will then quickly sell the stock at a high profit.[68]

Child pornography also underscores the international aspect of cyberspace, which permits transactions to occur when the buyer and seller are thousands of miles apart. Criminal activity is thus multijurisdictional, making law enforcement tougher. For example, in 1997 a major computer child pornography ring operating in twenty-one countries was uncovered. To bring law enforcement to bear on the ring required an unprecedented level of cooperation between the police and investigators in many different countries.[69] Child pornographers may seek haven in countries that have no laws against child pornography or no laws against the extraterritorial distribution of such material. If so, the U.S. Government will have an increasingly difficult time trying to gain jurisdiction over such defendants, who need not even physically set foot on American soil to distribute materials here.

Through computers, the way in which child pornography is produced may be altered as well. Obviating the need to find live children, producers may use their computers to draw such images from scratch or may digitally alter photographs of clothed children so that they appear nude. The question whether the law should extend to depictions that do not involve live children forces us to confront its very purpose: whether the law exists solely to protect minors, or, among other things, to prevent related molestation, or because child pornography is immoral.[70]

---

[68] For example, in April 1999, an e-mail posted on a Yahoo! message board under the subject line "Buyout News" said that PairGain, a California company, was being taken over by an Israeli company. DOJ REPORT, *supra* note 5, at 1. The e-mail also provided a link to what appeared to be a web site of Bloomberg News Service, which in turn contained a lengthy story on the purported takeover. As the news spread, the company's stock increased by more than thirty percent, and the trading volume grew to nearly seven times its norm. Yet the story was false, and the web site was not actually Bloomberg's site. When the hoax was uncovered, the stock plummeted. *Id.*

[69] The operation simultaneously executed search warrants in seventeen countries. DOJ REPORT, *supra* note 5, at C-1 n.3.

[70] Federal law currently forbids the distribution and possession of child pornography, and the prohibition specifically includes computers. 18 U.S.C. §§ 2251-2260 (1994 & Supp. IV 1998). Even if the image is not one of an actual naked child, but rather a computer-morphed or -manipulated image, it violates federal law. *See* 18 U.S.C. § 2256(8) (Supp. IV 1998) (defining "child pornography" to include any visual depiction of a minor engaging in sexually explicit conduct "whether made or produced by electronic, mechanical, or other means," and even if it "has been created, adapted, or modified"). The U.S. Supreme Court has recently granted certiorari to

The example of child pornography also sheds light on some of the intermediate parties that exist in cyberspace. In particular, an ISP may be used to transfer child pornography from one person to another, particularly when the internet is used to create mass distribution postings. For this reason, criminal law may usefully enlist ISPs to aid in enforcement. Indeed, federal law currently requires ISPs that become aware of an apparent violation of any federal child exploitation statute to report the violation.[71] In addition, law enforcement is currently permitted to subpoena an ISP to provide subscriber information to ascertain the identity of a child pornographer who lurks behind the veneer of anonymity.

The net can also make it easier to be an informant. In realspace, those with information about potential crimes are often afraid to give that information to the police. Retaliation may ensue against one's family, health, or property. Cyberspace can help prevent such retaliation; not even the police, let alone the criminal, knows who gave a tip. Moreover, tipping is as easy as writing an e-mail. Partially for these reasons, the federal web site for child pornography tips, CyberTipline, has received more than 8000 tips—in *two* years.[72]

Moreover, cyberspace partially melts the boundary between public and private enforcement by enabling citizens to become not simply informants, but also private enforcement agents. Take the example of a forty-five-year-old housewife in Pennsylvania who routinely surfs the net posing as a fourteen-year-old girl to see if she can trap a potential pedophile.[73] She turns information she gathers over to the police, who use it to open an investigation and bring a case.[74] The mother is

---

decide whether this law comports with the First Amendment. *See* Reno v. Free Speech Coalition, 198 F.3d 1083 (9th Cir. 1999), *cert. granted sub nom.* Ashcroft v. Free Speech Coalition, 121 S. Ct. 876 (2001).

[71] *See* 42 U.S.C. § 13032(b)(1) (Supp. IV 1998) ("Whoever, while engaged in providing an electronic communication service . . . obtains knowledge of [a violation of federal child pornography law] shall, as soon as reasonably possible, make a report . . . to a law enforcement agency."); *see also* Child Abuse Reporting Designations and Procedures, 28 C.F.R. § 81.1-.5 (2000) (designating agencies authorized to receive and investigate reports of child abuse).

[72] DOJ REPORT, *supra* note 5, at C-5. The internet can also help law enforcement develop a positive image in realspace. One police officer has created a web site dedicated to New Orleans's Community Policing Initiative, and the site has been credited with fostering better interactions between the police and residents. *See* Leslie Williams, *Officer Takes Community Policing to Cyberspace*, NEW ORLEANS TIMES-PICAYUNE, May 2, 1996, at A1. Such a web site may permit better extraction of information from tips and reports of illegal activity.

[73] Maria Glod, *Mom Hunts Pedophiles on Internet*, WASH. POST, Apr. 10, 2000, at A1.

[74] *Id.*

able to pose as a girl due to the invisibility of the internet—with no training.[75] In realspace, such posing would present significant obstacles; someone with the necessary maturity would need to appear to be younger than she is and would have to be taught physical defense techniques to prevent retaliation should the suspect uncover the ruse. By contrast, in cyberspace, everyone can play this role, for better or worse.[76] Indeed, CyberAngels—a 4000-member offshoot of the Guardian Angels—patrols cyberspace for stalkers and child pornography, and brings its findings to the police.[77] The CyberAngels operate invisibly and electronically record each move of their suspects. This raises numerous questions, from whether there is a proper role for private citizens in law enforcement to whether police investigations will be hindered when overlapping entities—both private and public—are performing similar roles.[78]

2. Copyright

Cyberspace has transformed intellectual property theft. Imagine, for reasons best unknown, that it is 1980 and you want to pirate Journey's "Escape" album. You would have to buy a legitimate copy, buy expensive recording equipment to copy the album to tape or audiocassette, and also reproduce the album cover and other accompanying material. The whole process would be enormously difficult. Copies of copies degrade quickly and have poor quality, but without them, you would be stuck replaying "Escape" all the time (at some cost to your sanity), and only able to copy the album about

---

[75] Invisibility, however, is contingent upon the architecture of the net and other factors, such as the cost of video and biometric devices.

[76] My claim is not that such private action is impossible in realspace, only that it is easier due to the advantages of cyberspace. Certain laws, such as Megan's Law, also attempt to turn realspace citizens into deputy police officers by placing them in the position to monitor convicted sex offenders. *See* Abril R. Bedarf, *Examining Sex Offender Community Notification Laws*, 83 CAL. L. REV. 885, 903-06 (1995) (describing the emerging trend of community notification of sex offender registration whereby "individuals may police their own communities to *prevent* sex crimes").

[77] Glod, *supra* note 73 ("Thousands of volunteers worldwide have been rising up to combat child pornography, stalkers and sexual predators on the Internet.").

[78] To take one example, a federal agent posed as a thirteen-year-old girl in a chat room and an internet relationship eventually evolved between the agent and a middle-aged man. DOJ REPORT, *supra* note 5, at C-6. They made plans to meet in realspace, but the man postponed the meeting because he stated he was meeting another underage girl. Out of concern for the new girl's safety, the agent requested an arrest warrant for a lesser charge of conspiracy. The next day, the agent discovered that the "victim" was an undercover officer from another state. *Id.*

twenty-five times per day. Once you have your copies, you then would have to decide how to sell them. Typically, the goods would be sold to a wholesaler, who would then sell them to a retailer. (You, as the producer, do not have the time to break away from flipping the album over and over to sell the copies yourself.) But selling on the street is highly visible; the police may see your operation and shut it down. Moreover, the structure of the distribution scheme facilitates law enforcement infiltration, whereby, for example, the police obtain the cooperation of the retailer to make a case against the wholesaler, and then use the cooperation of the wholesaler to make a case against the person doing the copying.[79]

In short, analog degradation, high copying costs, and the risk that your co-conspirators will be flipped are hallmarks of the offline distribution scheme. But not in the computer age. Even copies of copies are now almost perfect. Copying costs are nil; you can simply download the album once to your computer and post the material once on the internet. Within minutes, your album could be distributed across the planet. You would not need to bother with wholesalers, retailers, and the like; you would be self-made, with no one to extract extra costs or finger you down the road. Nor can your customers—none of whom have ever seen you or know any personal details about you—identify you. And even if law enforcement infiltrated your site, they would not necessarily know your true identity.[80]

This is not the world of fiction. Even before the MP3's popularity, in 1998 music piracy caused an estimated loss of $300 million.[81] And that year, before the advent of widespread distribution technology, software piracy cost the United States some 109,000 jobs and $991 million in tax revenue.[82] Microsoft lost more than $500 million last year due to software theft. With Napster and the rise of other innovative distribution systems, these numbers will only get worse.[83]

---

[79] *Id.* at I-1.

[80] Information, once unleashed on the internet, has the characteristics of a public good in that it is tremendously nonexcludable and nonrivalrous. But as America has recognized since its founding, intellectual property rights must be preserved in order to provide incentives to create new works.

[81] DOJ REPORT, *supra* note 5, at I-2. These numbers may be inaccurate insofar as they may (1) undercount or overcount the possibility of undetected piracy, (2) assume every pirated copy would have been sold, and (3) underestimate fair use.

[82] *Id.*

[83] In December 1997, Congress passed the No Electronic Theft ("NET") Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997) (codified as amended in scattered sections of the

I want to take two aspects of copyright theft to foreshadow my claims in this paper. The first concerns the role of profit in criminal enterprise. In realspace transactions, the pirated CD is sold for relatively untraceable cash on the street. In cyberspace, however, no adequate profit model exists for pirates. The easiest way for a pirate to get paid is through credit cards. But credit card transactions are traceable. Law can harness credit card companies in the fight against cybercrime by changing payment rules. For example, if law gave cardholders the right to refuse to pay bills derived from illegal transactions, credit card companies would scrutinize members of their credit networks. The idea is to alter the profit stream from criminal activity rather than the expected criminal sanction.

Second, because computer copyright crimes lack a hierarchical distribution scheme, it is unlikely that law enforcement will find witnesses to "flip" and use as cooperators who can inform on, or testify against, the key culprits. In cyberspace, everyone is a potential big fish, and the smaller fish—who might, in realspace, become cooperators—have disappeared. As a result, the law should be rethought. To the extent that Congress imposes high penalties on

---

United States Code), in an attempt to prevent theft of copyrighted materials. Under the Act, the unauthorized distribution and reproduction of copyrighted works is a felony, punishable by up to five years imprisonment. 18 U.S.C. § 2319(b)(1) (Supp. IV 1998). Strikingly, the Act punishes distribution regardless of whether the distributor was trying to profit from it. 17 U.S.C. § 506(a)(2) (Supp IV. 1998); 18 U.S.C. § 2319(c) (describing the punishments applicable to a violation of § 506(a)(2)). Thus, even if the material was placed on one's web site solely for pleasure—as a way of indicating to friends what you are listening to this month—the law is violated.

The legislation was designed to remedy the purported defect in the criminal copyright statute highlighted in the dismissal of an indictment in *United States v. LaMacchia*, 871 F. Supp. 535 (D. Mass. 1994). In *LaMacchia*, an MIT student operated a bulletin board that allowed anyone to send or acquire copyrighted software programs. The student's actions caused an estimated loss to copyright holders of over one million dollars during the six-week period the system was in operation. *Id.* at 536-37. The student could not be charged with violation of the criminal law protecting copyright, 17 U.S.C. § 506, because he was not acting for commercial purpose or private financial gain, an element of the criminal copyright offense. *See LaMacchia*, 871 F. Supp. at 542-43. Instead, he was charged with conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1343. *LaMacchia*, 871 F. Supp. at 536; *see also id.* at 541-42. The district court dismissed the indictment, finding copyright law to be the exclusive remedy for protecting intellectual property rights from this kind of theft. *Id.* at 545. In an example of prescriptive advicegiving, the district court invited Congress to remedy this gap in the law. *See id.* ("One can envision ways that the copyright law could be modified to permit such prosecution."); *see also id.* ("In sum, I agree with Professor Nimmer that... 'absent a clear indication of Congressional intent, the criminal laws of the United States do not reach copyright-related conduct.'" (quoting 3 NIMMER ON COPYRIGHT § 15.05, at 15-20 (1993))).

minor crimes undertaken by smaller actors to induce these actors to flip (and not because of the underlying harmfulness of the acts), these penalties may have to be modified. And to the extent that prosecutorial tactics are derived from an impetus to flip witnesses, these tactics may need modification too. Rather, punishment may need to turn on the harmfulness of the underlying act.

Is there, then, no role at all for informants and cooperators in cyberspace? On the contrary, the role should persist, but in a different form. Current federal law generally permits downward sentencing departures only for those who provide information about an ongoing criminal case;[84] cybercriminals who have tried to seek a lower sentence on the basis of cooperation with law enforcement to prevent future attacks have been spurned.[85] But this policy should be changed, for this type of cyberspace cooperation carries social benefit that makes it just as, if not more, valuable than traditional realspace cooperation in which culprits are fingered and inculpated.[86] Because cybercrime is so easy to commit, and much of the knowledge needed to make it more difficult resides in private hands, government must devise methods to extract such information from criminals. This is an application of cost deterrence once again. The use of informants to help design better computer systems and prevent crimes from occurring is unlike the use of flipped witnesses in realspace. It portends a proactive, not reactive, model of law enforcement.

3. Cyberstalking

Cyberstalking occurs when someone is threatened or harassed online. The Justice Department believes that there may be hundreds

---

[84] *See* U.S. SENTENCING GUIDELINES MANUAL § 5K1.1 (1998) (allowing courts to depart from the sentencing guidelines if "the defendant has provided substantial assistance in the investigation or prosecution of another person who has committed an offense").

[85] *See* Interview with Jennifer Granick, Criminal Lawyer (May 2, 2000) (stating that in the course of defending many cybercriminals, she has requested such a departure but it has always been refused). The famous phone phreak Captain Crunch, who broke into most telephone systems in the 1970s, tried to get a lighter sentence by revealing the extent of his assistance to the government. He claimed that he had "volunteered to help the government plug leaks in its phone and computer systems." PARKER, supra note 18, at 176-77. The court, however, refused his request. *Id.* at 177.

[86] The government has tried to recruit hackers to help it develop secure countermeasures, even as recently as August 2000. *See* Schwartz, *supra* note 24 (describing the Pentagon's recruitment efforts at the annual Def Con hackers convention).

of thousands of cyberstalking incidents each year.[87] Stalking is nothing new, but cyberstalking has some new features. An anonymous stalker is harder to catch. Because the perpetrator does not see the harm his actions inflict, the victim's reaction cannot cause a change of heart. The lack of an in-person confrontation also makes intent harder to presume or ascertain.

Current federal law makes it a crime to transmit any communication in interstate or foreign commerce—including communication over the internet—containing a threat of personal injury.[88] And a separate statute makes it a crime to use a telecommunications device anonymously to annoy, abuse, harass, or threaten any person.[89] The latter statute, however, applies only to direct communications between perpetrator and victim and does not apply to situations in which a perpetrator posts messages encouraging third parties to harass or annoy a victim. For example, last year a former security guard pled guilty, under California law, to stalking and solicitation of sexual assault for using the internet to solicit a rape. A woman had rejected the guard's romantic overtures, and, in retaliation he impersonated her in chat rooms, posting her phone number, address, and fake messages detailing how she fantasized about being raped. As a result, on at least six occasions, at times late at night, men knocked on her door saying they wanted to rape her.[90]

How should the law think about this semiconspiracy between men? There is often an implicit collusion between the publisher of the message and the viewers of that message, as the example above suggests. Take another real example, drawn from copyright: Is it a conspiracy when a student places copyrighted programs on his web site that may be copied by others?[91] On the one hand, there is no real conspiracy between the publisher and the viewer, as no true meeting of the minds can be said to exist. It is difficult to know whether the student intended for further copying to occur. On the other hand, however, we can be sure he knew such further copying was possible, for he had done it himself and thus knowingly created an opportunity

---

[87] *See* U.S. ATTORNEY GEN., 1999 REPORT ON CYBERSTALKING: A NEW CHALLENGE FOR LAW ENFORCEMENT AND INDUSTRY (1999), *available at* http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm [hereinafter CYBERSTALKING REPORT].

[88] 18 U.S.C. § 875(c) (1994).

[89] 47 U.S.C. § 223(a)(1)(C) (1994).

[90] DOJ REPORT, *supra* note 5, at 10.

[91] In one highly publicized case, David LaMacchia was indicted for one count of conspiring "with persons unknown" to violate the federal wire fraud statute. *See supra* note 83.

for numerous others to commit the same act. If the law seeks to deter crime by foisting incentives for crime prevention on those in the best position to undertake it, then one must consider whether liability should be placed not only on those who post the messages but also on those who host the messages: ISPs. Current federal law specifically exempts ISPs from liability for cyberstalking, but perhaps this provision needs to be rethought.[92]

The security guard example provides one illustration of complementarity between cybercrime and crime in realspace. Another example occurs when cyberstalkers escalate their behavior into realspace stalking. The DOJ believes that, "as with physical stalking, online harassment and threats may be a prelude to more serious behavior, including physical violence."[93] Anecdotal evidence suggests similar complementarity in pedophilia cases as well, where cybersex has escalated into attempts at actual sex.[94]

To the extent that the online world shapes tastes that eventually culminate in realspace behavior, the law and internet institutions may need to act. Even if there is no causality between cyberstalking and realspace stalking, the two acts may still be heavily correlated. That is, those who cyberstalk may also be likely to engage in realspace stalking. If evidence in cyberspace is easier to gather (for example, the permanent record left by a posting may be easier for law enforcement to obtain than the footsteps heard by a victim in the dark one night), the law might criminalize cyberstalking for two reasons, regardless of whether cyberstalking is itself harmful. First, cyberstalking investigations could provide evidence that would constitute probable cause to search an apartment for evidence of realspace stalking.

---

[92] "The definition of the term 'telecommunications device' in [47 U.S.C. §] 223 excludes 'interactive computer services.' The intent of the exclusion is to insulate the service provider from liability." CYBERSTALKING REPORT, *supra* note 87, at n.10.

[93] *Id.* It is possible that cyberstalking might function in some circumstances as a substitute for stalking in realspace. This function would suggest that cyberstalking ought to be legalized to prevent realspace stalkings (which are more harmful). I know of no evidence that supports this point.

[94] *See* Jo-Ann M. Adams, Comment, *Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet*, 12 COMPUTER & HIGH TECH. L.J. 403, 414 & n.74 (1996) (discussing the harm to children who "have been lured from their homes and molested based on conversations in chat rooms on the Internet"); Barbara Kantrowitz, *Child Abuse in Cyberspace*, NEWSWEEK, Apr. 18, 1994, at 40 (discussing the arrest of men who used the internet in furtherance of their plans to molest children physically); Vincent J. Schodolski, *Online Anonymity Conducive to Vice*, CHI. TRIB., June 11, 1995, at 19 (describing various men who met young children and teenagers online and used their computers to arrange meetings in realspace that eventually culminated in rape).

Second, cyberstalking investigations could allow police to alert a cyberstalker that he or she is under suspicion and should curb his or her behavior, particularly in realspace.[95]

4. Illegal Firearms Sales

The sale of illegal guns shares many of the features of cybercrime we have already discussed: Anonymity facilitates transactions and frustrates the ability of law enforcement to recruit informants and cooperators, and invisibility allows evasion of law enforcement (through, for example, use of a private, password-secured chatroom).[96] Gun sellers in cyberspace cannot conduct a trustworthy background check even when legally required to do so. Furthermore, cyberspace, due to its potential to bring people of like minds together, will facilitate the meeting of illegal buyers and sellers in the first place, despite the fact that they live in different states or even in different countries. These facts do not make computerized gun sales impossible to regulate because law enforcement may monitor chatrooms and because the purchased guns must still be delivered in realspace. On balance, however, law enforcement in this area is more difficult in cyberspace.

Many cyberspace gun sales are detectable to at least one third party: the web site or ISP involved. Accordingly, there may be room to require ISPs and web sites that permit such transactions to monitor them and to ensure their compliance with the law.[97] There may be private enforcement as well: web sites may refuse to permit gun transactions (eBay currently maintains such a prohibition) or may monitor customers through sophisticated realtime word searches. These private countermeasures raise two questions: (1) How much private, rather than public, law enforcement is optimal? (2) How

---

[95] The two points here, about the use of sweeping criminal laws to maximize government search power and to create warning effects, are of general applicability and contradict the standard notion in criminal law that punishment should be calibrated to the harmfulness of an act.

[96] DOJ REPORT, *supra* note 5, at E1-E3.

[97] For example, the Internet Gun Trafficking Act of 1999, S. 637, 106th Cong., introduced by Senator Schumer in March 1999, would require web site operators who allow advertisements of firearms sales on their sites to obtain a license and to prohibit buyers and sellers who access a licensed web site from identifying themselves to each other (to keep them from evading the licensed operator by directly contacting one another). It would require the web site to act as an intermediary to process the transaction and ensure that the buyer and seller do not evade applicable legal requirements.

should these two types of enforcement be structured?

The four examples discussed thus far reveal the many similarities between cybercrime and traditional criminal activity. Some of what we call cybercrime is simply ordinary crime, and the use of a computer is merely incidental to the criminal scheme. Nevertheless, these similarities should not blind us to the significant differences between cybercrime and crime in realspace.

II. TREATING CYBERCRIME DIFFERENTLY

A. *First-Party Strategies*

1. Five Constraints on Crime

Criminal law is not a species of law designed only to remedy past wrongs; it also directs its attention to deterring future wrongdoing.[98] Legal scholars have recognized three main forms of regulation of criminal behavior: law enforcement risks, social norms, and architecture. Social norms strategies emphasize that police are not always present and that internal morality (conscience) and external enforcement (shaming) can deter crime. Architectural strategies change the electronic and physical layout in ways that make crime more difficult to carry out. Public spaces can be configured to maximize visibility and ensure detection, and computer software can be coded to control its use.[99] Note that norms and architecture do not

---

[98] *See* Katyal, *supra* note 10, at 2421 n.118, 2427-29 (citing empirical evidence for the effectiveness of deterrence); Daniel Kessler & Steven D. Levitt, *Using Sentence Enhancements To Distinguish Between Deterrence and Incapacitation*, 42 J.L. & ECON. 343, 359 (1999) (finding that California's recent sentencing enhancements increased deterrence and that they "may represent an effective means of reducing crime"); *see also* Dennis Director, *Law and Order for the Personal Computer*, *in* COMPUTERS UNDER ATTACK, *supra* note 55, at 528, 546 (describing how a former computer fraud artist "stopped hacking when he concluded that the penalties were too severe"); David Landis, *Sex, Laws & Cyberspace*, USA TODAY, Aug. 9, 1994, at 1D (stating that the conviction of Robert and Carleen Thomas for distributing pornography online "hit the on-line community like a cold shower" and quoting one adult Bulletin Board operator as stating, "Everybody is scared .... We wish we knew what the rules are. If I knew what the rules are, I certainly would follow them."). Deterrence may work better in cyberspace because information costs are lower, making it easier for criminals to learn about the law and its enforcement.

[99] In realspace physical architecture is also employed to prevent crime, such as locks on doors and safes, and light to prevent nighttime burglaries. *See, e.g.*, C.J.H. Woodbury, *The Barbarians of the Outside World*, ELECTRICAL REV., Apr. 30, 1887, at 2 ("[E]xtinguish the electric light while the sun is beneath the nadir, and crime would riot.").

necessarily require an offender to know the risk of getting caught or the legal sanction involved. Thus, these forms of deterrence can still work for those with utter disregard for, or ignorance about, the law.

Another constraint that creates deterrence regardless of knowledge about the law is the physical risk from crime. One cost of consuming illegal drugs is the health consequences (ranging from illness due to substance adulteration to addiction). Robbing a bank in realspace is not simply a matter of dollars and cents; it also risks physical violence to the perpetrator, the bank officers, and the public.[100] Reliance on physical risks to control crime raises troubling moral issues and lacks the advantages of other constraints (such as certainty of imposition). Nevertheless, the variable must be understood, if for no other reason than to use it as a predictor of crime. For example, one can predict that the incidence of computer crime will rise compared to realspace crime because the former has lower physical risks due to the invisibility and remoteness of cyberspace.

In cyberspace, there are ways to adjust strategies that rely on physical risk to minimize the moral problems. For example, the law might authorize victims of cybercrime to retaliate against a perpetrator's software and hardware, and such retaliation might be confined to imminent self-defense. Alternatively, the law might enable a broader right (such as permitting victims to install nonreplicating viruses in perpetrators' systems several days after an attack).

My claim in this Part is that criminal law scholars should concentrate not only on legal sanctions and physical risks but also on ways to increase the expense of committing crimes. This is the notion behind cost deterrence.[101] If robbing a house and robbing a store

---

[100] Some forms of deterrence consciously harness these physical risks, such as the INS's recent strategy to close the flatlands border with Mexico, but leave the dangerous mountain passes unguarded because the risk of death provides an adequate deterrent. Susan Ferriss, *Fox Seeks New Solution to Old Border Problems*, AUSTIN-AM. STATESMAN, Aug. 20, 2000, at A1.

The aforementioned bank robbery example also forces us to understand what act we are punishing and why. To the extent that a crime is penalized in a certain way because of the risk of physical violence, similar acts in cyberspace may merit a lower penalty. If bank robbery is punished by a minimum of five years because of the theft and because of the risk of physical violence accompanying the theft, a cybertheft might receive less than five years because only one of these two variables is present. Law must then weigh the harmfulness of the act apart from its complementary crimes.

[101] If the price of burglars' tools increases by $100, monetary costs increase but law enforcement risks do not. Conversely, if police develop a way to tap and pinpoint cell

produce equal profit, but the latter requires much more investment by the criminal (in casing the store, hiring lookouts, etc.), the expected sentence for the house robbery should be greater. Law should capitalize on these costs and use them to maximize deterrence. Price has been neglected by economists; even the writing in the wake of Becker's famous article equates law enforcement risks with higher cost, without discussing monetary cost as a deterrent.[102] If the law can raise the cost of criminal activity to a would-be perpetrator, it may deter some of that wrongdoing in the first place. Unlike the speculative cost of prosecution, which criminals may wrongly discount due to poor judgment about risk, criminals are certain to incur these up-front monetary costs.

Because offenders vary in age, social standing, averseness to risk, and income, the other constraints outlined above may prove useful. Legal sanctions may be particularly effective at deterring wrongdoing when offenders are relatively risk averse. They may also be effective in deterring those individuals who invest in their reputations—who fear the social stigma of lawbreaking.[103] There are, however, other circumstances in which expected sentences should not be raised, such as when diminishing returns exist or when higher sanctions seem cruel and disproportionate and therefore immoral or unconstitutional.[104]

---

phones, the law enforcement risk is raised while the monetary costs of crime may not be—at least until an expensive untraceable cell phone is built and monetary costs are raised. These examples demonstrate, however, that the line between monetary costs and law enforcement risks is not always clear. Law enforcement risks can give rise to monetary costs, and vice versa. A criminal may respond to the law enforcement risk of phone taps by paying the extra monetary costs incurred by using secure phone lines or the mails, just as a thief may need to borrow money from a third person to cover the increase in the price of burglar's tools, and this third person may be induced to cooperate with law enforcement.

[102] Standard models of deterrence, such as those of Gary Becker and George Stigler, focus not on cost deterrence, but on law enforcement risks (specifically, the probability of being caught and the sanction imposed). Becker, *supra* note 6, at 169-95; George J. Stigler, *The Optimum Enforcement of Laws*, 78 J. POL. ECON. 526, 527 (1970).

[103] Stigma is only partially related to the length of sentence; there is a large discontinuity between legal activity and activity that is illegal but which only merits low amounts of jail time. For this and other reasons, there are diminishing returns to larger sentences.

[104] Generally speaking, just as with the other forms of constraint, monetary cost is endogenous to the way in which law treats a given act. If an act is punished, the supply of those offenders willing to commit the act may drop, and thus increase the cost of inducing someone to commit it. The threat of legal sanctions may also force criminals to incur monetary costs to avoid detection (from physical disguises to stealth software

This is where the other constraints come in. For example, changing a twenty-year sentence to twenty-five years for a particular crime may have little effect on the criminal, whereas changing the actual monetary costs of commission of the crime may significantly promote deterrence. This is particularly so when law is trying to deter a population of offenders that are relatively prone towards risk. Computer crimes, for example, tend to be committed by reckless youths who worry much less about jail time than about their social standing and the money in their pocket.[105] Increasing legal risks is a somewhat bizarre way to deal with this problem. Instead, crimes could be made more expensive by taxing dangerous software, charging small admissions fees to enter sensitive web sites, and so on. If web sites adopt fees for service, such as Napster, those fees might prevent more criminal acts than would an increase in legal penalties because teenagers are more sensitive to monetary price than legal risks. Solutions that rely on social norms may also prove effective. Schools could try to foster good computer practices and explain the harm of computer crime to students. They can stigmatize offenders by doling out punishments that produce shame, such as making them clean bathrooms in orange jumpsuits and the like.

Across the broad field of criminal law, the heterogeneity of offender populations plays out in other ways besides attitudes towards risk. Perpetration costs will act as a larger constraint for poorer offenders.[106] When offenders are sensitive to their social standing, strategies that rely on social norms and law enforcement risks will have a greater impact.[107] When offenders lack legal knowledge or understanding of social mores, strategies that rely on architecture may be more effective than those that rely on law. When offenders have technical expertise that allows them to pierce architectural solutions, then other constraints such as price and norms may be more effective.

---

and hardware). Monetary costs are often also endogenous to social norms and architecture. If society condemns a certain act, the cost of getting someone to commit it will be greater, and those who commit it will expend funds to avoid detection by society. Furthermore, if code prevents criminals from carrying out certain forms of crime, criminals may expend resources to hack the code.

[105] *See, e.g.*, Fiona Harvey, *Hackers Chip in at Digital Security Event*, FIN. TIMES, Nov. 4, 2000, at 5 ("Some kids think they can hack into a network, get caught, not do a jail term because they're minors, and walk into a six-figure salary as a security expert.").

[106] *See* Katyal, *supra* note 10, at 2416-19 (discussing how the price of a crime, rather than the crime's attendant jail term, may be a greater deterrent for people with lower incomes).

[107] *See id.* at 2416 ("People who 'invest' a great deal in their reputations are likely to forgo utility-producing acts that tarnish their social standing.").

Many other variables will affect the choice of which strategies to use in a given instance; these include the technical ability to detect and catch criminals (high ability favors reliance on legal sanctions, while low ability favors architecture) and the need for public governmental judgment in applying the rule (which leads to the use of legal sanctions and prosecutorial discretion), as opposed to nongovernmental private judgment in application (which leads to a focus on norms).

Accurate assessments of optimal deterrence, therefore, should go beyond legal sanctions to incorporate concepts of monetary cost, social norms, physical risks, and architecture. Each strategy has important distributional consequences and will target a different population of offenders. As we shall see, however, they often carry unique costs as well.

2. The Efficiency of Cybercrime

The advent of personal computers poses a significant threat to the rule of law. That is because: (1) computers are a powerful substitute for additional people in a criminal enterprise; (2) computers permit anonymity and secure communications; and (3) cybercriminals are often invisible, remote, and untraceable. Computers therefore have the potential to reduce all five constraints on crime. With computers, crime is cheaper to commit and criminals find it easier to escape detection and apprehension.[108]

a. *Conspiracy's Demise*

Before computers, a criminal typically needed to work with other individuals to conduct serious criminal activity. Group crime arose for obvious reasons, from economies of scale to specialization of the labor pool. For example, it is nearly impossible for one person to rob a bank successfully. Several individuals are needed to carry weapons

---

[108] Many suggest that computers also help law enforcement because they allow the police to coordinate and organize information. In general, the bulk of these advantages accrue regardless of whether the crime takes place in cyberspace or realspace. The advantages, therefore, do not affect my claim that cybercrime is generally a cheaper way for a criminal to act. *See* Telephone Interview with Cliff Stoll (May 1, 2000) ("There is no question that online crimes are much easier to commit than offline ones."). The two advantages computers provide to law enforcement that are unique to cybercrime are electronic tracing and powerful data searches. Both of these advantages, however, are currently of dubious value to law enforcement. *See infra* Part II.A.2.c.

and provide firepower (economies of scale); someone needs to plan the operation (a form of specialization of labor); another must serve as a lookout (specialization again); and many people are needed to carry the money. Working together with others, whether in the criminal or corporate world, creates obvious efficiencies, as Ronald Coase explains in his pathbreaking article about why firms develop.[109]

But computers change all this, and undermine the need for criminal conspiracy. As discussed in Part I, a cyberthief can, by herself, design a program to steal money from an electronic bank account or data from the Defense Department, rather than enlist a team to do so. A fraud artist can, by herself, send thousands of e-mails to unsuspecting recipients to create a Ponzi scheme. A child pornographer can create, store, and distribute images, and receive royalties or access fees without assistance. In these situations, a computer enables a single individual to launch a crime: No individual in realspace could break and enter a physical premise, and remove and steal the classified material without detection, perpetrate all the aspects of a Ponzi scheme, or run a child pornography ring. Cyberspace, however, is different. The electronic walls that secure money and data are pierced, not by additional thugs, but, rather, by additional computer power. In addition, cyberspace avoids the physical constraints of realspace (a burglar can only carry away a certain amount of loot and be in one place at a time).

Compare a computer to a co-conspirator, and the choice for even a dim criminal is obvious. A computer can conduct many of the tasks that co-conspirators used to undertake, from breaking and entering, to managing assets and inventory, to keeping accounting records. Additionally, a computer, unlike a co-conspirator, acts selflessly in that it does not demand a percentage of the rewards from criminal activity, and it is always loyal, without any bonding costs. A computer will not betray a criminal's confidences—either to law enforcement or to other criminals.[110] (Not only are co-conspirators flipped, conspiracies often yield tangible evidence for law enforcement, including phone records between co-conspirators, wiretap information, and overheard

---

[109] *See* Ronald Coase, *The Nature of the Firm*, 4 ECONOMICA 390 (1937), *reprinted in* FOUNDATIONS OF THE ECONOMIC APPROACH TO LAW 61 (Avery Wiener Katz ed., 1998).

[110] The Supreme Court has recognized that a "genuine privilege . . . must be recognized for the identity of persons supplying the government with information concerning the commission of crimes. Communications of this kind ought to receive encouragement." McCray v. Illinois, 386 U.S. 300, 308 (1967) (citing 8 WIGMORE, EVIDENCE § 2192 (McNaughton rev. 1961) (emphasis omitted)).

conversations.) Computers also provide the near-perfect security afforded by encryption; not only will they not choose to talk, but computers will not be able to talk even if "interrogated."[111] Faced with the choice between a computer that will not betray them and a live person who might, criminals will pick the computer. These numerous advantages make computers safer for criminals than additional co-conspirators. In economic terms, computers are a shift from labor-intensive to capital-intensive strategies and boast all the benefits of the latter.

Thus, put most provocatively, old-fashioned conspiracy—costly and susceptible to detection—is a good thing for law enforcement because it raises monetary costs and law enforcement risks. Admittedly, criminals in a conspiracy egg each other on, thereby encouraging further criminal activity,[112] while computers, by contrast, do not. Nevertheless, the benefits that computers provide to individual criminals outweigh the limited magnification that occurs from group crime. For this reason, criminal law might want to penalize the use of a computer in crime. If the law treats an agreement between Jones and Smith to engage in illegal activity as a crime, why should it not equally treat Jones's use of a computer as a species of crime? By substituting a computer for co-conspirators, a culprit in a sense simply chooses to conspire with his computer. This fact might justify treating a computer as a living entity, just as a corporation is treated as a living entity in other areas of law, and suggests that Jones should be punished for engaging in a quasi-conspiracy with his computer. Federal law already punishes the use of the mails and wires to facilitate a criminal offense; these technologies are ones that permit co-conspirators to act in concert and magnify their power.[113] Computers are an even more powerful mechanism for engaging in crime and their use also justifies the creation of a separate

---

[111] In one respect, computers may be less reliable than co-conspirators. If a criminal records her activity on the computer, and law enforcement has the ability to read it (by breaking the encryption regimes), a computer has no free will that would prevent it from letting the police read and access those records. A human co-conspirator, by contrast, may refuse to cooperate and may "forget" damaging details. The growth of powerful encryption that law enforcement cannot crack, however, *see infra* Part II.A.2.b, as well as the difficulty involved in finding a criminal loyal enough to an enterprise to refuse to cooperate in the face of significant jail time, means that computers on balance are far more helpful than the bulk of additional co-conspirators.

[112] *See, e.g.*, United States v. Rabinowich, 238 U.S. 78 (1915); *Developments in the Law—Criminal Conspiracy*, 72 HARV. L. REV. 920, 924-25 (1959) [hereinafter *Developments*].

[113] 18 U.S.C. §§ 1341, 1343 (1994).

crime.[114]

One might object that a computer is not really like a co-conspirator because, unlike a person, it can never be induced by a sentencing departure to turn into a voluntary informant or cooperator. The objection would stick if conspiracy law were only intended to aid in extracting information from co-conspirators, but it is not. Conspiracy law is primarily intended to punish and deter conspiracies. Ironically, however, if the law sought to gain information from conspirators, it should *encourage* conspiracies to form and then devise mechanisms to harvest information from members of the group.[115] Of course, this is not how the law works.

One might also object that the reason conspiracy is penalized is that co-conspirators are bad men who convince each other to ignore their consciences. That is why conspiracy is an inchoate crime—the agreement itself is immoral, on this theory, even before it produces harm. And there is no immorality in a computer's lending itself to use in a crime; for it has no free will to refrain—so a computer is hardly similar to a co-conspirator. The problem with this line of reasoning is that the law cares not only about the agreement, but also about its harms, so that a conspiracy to sell a marijuana cigarette receives a much lower penalty than a conspiracy to blow up a building—for the level of punishment for conspiracy slides with the object of the conspiracy.[116] This sliding provision suggests that conspiracy law may be motivated, in part, by the desire to deter the most harmful conspiracies from forming.

---

[114] There are other items, such as guns, that may also reduce the number of conspirators necessary to commit a crime. Law generally punishes the use of these items separately through sentencing enhancements and specific exclusions. *See infra* text accompanying notes 146-66. Computers, however, will generally have a multifaceted relationship with a criminal that more closely approximates the relationship to a co-conspirator than a one-dimensional item like a gun will provide. Nevertheless, the substitution between guns and conspirators may be an important fact to consider in setting gun penalties.

[115] In a forthcoming work, I use this idea to suggest that the government can pay conspirators for information of criminal wrongdoing and that such payments should be given in a way that prevents law enforcement from knowing the identity of the person providing the information.

[116] The range of punishment for a conspiracy designed to undertake a particular act (such as to blow up a building) is the same range of punishment that faces an individual executing the act. For additional support for the view that conspiracy is grounded in utilitarian theory, see RICHARD POSNER, ECONOMIC ANALYSIS OF LAW 254 (5th ed. 1998) ("The special treatment of conspiracies makes sense because they are more dangerous than one-man crimes . . . in being able to commit crimes more efficiently . . . by being able to take advantage of the division of labor.").

If that is the case, then it makes sense to punish the use of a computer to carry out a crime as if the computer were a quasi-conspirator.[117] Doing so will deter the greater damage computer crime can incur per unit of investment in the enterprise. It will also redress the substitution effects created by the lopsided punishment of conspiracy in current law. In realspace, a crime accomplished with co-conspirators receives criminal liability for both the underlying offense and the conspiracy. The same crime, accomplished in cyberspace, triggers only liability for the underlying offense. The result is effectively to subsidize the use of computers in crime. The remedy is to recognize that, because computers are substitutes for co-conspirators, computer crime, like conspiracy, should trigger not only basic liability for the underlying offense, but also conspiracy-like liability for the use of computers in lieu of co-conspirators.

Treating computers as quasi-conspirators captures one of the main benefits of conspiracy law: it targets inchoate conduct. The *Model Penal Code* and its commentators justify realspace conspiracy doctrine on the ground that it permits the government to intervene against persons who are disposed to criminality.[118] Because the harm of computer crime is so great, providing government with a device to prevent this harm by those truly disposed to commit it may be socially optimal. The achievement of optimality would depend on whether government could minimize error costs. Realspace conspiracy doctrine's insistence on an agreement between real persons arguably creates two potential safeguards to minimize error costs: (1) co-conspirators can verify the existence of a conspiracy; and (2) the act of reaching agreement with another person may be a stronger signal of criminal intent than is typing some commands at a computer. Of course, the presence of additional persons might make error costs higher (those caught may unfairly blame innocents, unlike

---

[117] Intent doctrines derived from realspace, where high transaction costs make it difficult to persuade additional persons to join a conspiracy, may not apply in the low-transaction-cost world of using a computer for nefarious ends. In addition, the likelihood of harm from any single agreement between a computer and its user may be less than that resulting from any single agreement between two corporeal beings because the transaction costs are so low in the former setting. This may justify low punishments for inchoate cybercrime conspiracies.

[118] *See* MODEL PENAL CODE § 5.03 cmt. 1, at 387 (1985) (rationalizing conspiracy law as a means of addressing "preparatory conduct" and "the special danger incident to group activity"); Ian H. Dennis, *The Rationale of Criminal Conspiracy*, 93 L.Q. 39, 40-44 (1977) (explaining that a rationale for conspiracy is that it allows the law to intervene "before a contemplated crime had actually been committed"); *Developments*, *supra* note 112, at 923-25.

computers) and realspace conspiracies may be easier to stop than some computer crimes (such as viruses, which often spread far beyond a writer's wildest dreams). Nevertheless, this militates in favor of adopting a form of inchoate liability that attaches only once a very substantial step in furtherance of a computer crime has been taken.[119]

In sum, the law might develop penalties for using computers to aid a criminal offense. The case for criminalization proceeds from the fact that computers and co-conspirators are substitutes for each other. The solution proposed would not necessarily require treating computers as full co-conspirators, but it would require eliminating the law's current conceptualization of a computer as simply a method of crime, not a type of (or substitute for) a participant in crime.[120]

b. *Pseudonymity and Encryption*

Computers also confer massive efficiencies on the criminal by hiding the perpetrator's identity and covering data streams. Digital pseudonymity refers to the ability to cover one's true name while in cyberspace. For example, my e-mail signature may be nka9845@aol.com and my IP address may be a series of numbers that match only an ISP. Without the ISP's cooperation, it is nearly impossible to figure out who nka9845 is, and even more difficult to pinpoint nka9845's location in realspace. Even masked or otherwise disguised criminals in realspace may unwittingly indicate their height, race, voice, and now their DNA. All of this helps law enforcement in realspace, which is why police take so much time with witnesses,

---

[119] Current federal law requires proof of only an agreement and an "overt act" to sustain a conviction for conspiracy. 18 U.S.C. § 371 (1994); United States v. Lichenstein, 610 F.2d 1272, 1276 (5th Cir. 1980). Law could borrow from attempt liability, however, to impose a "substantial step" requirement before treating a computer as a quasi-conspirator. As a well-known treatise explains:

> [U]nder attempt law it must be shown that the defendant has taken . . . a 'substantial step' toward commission of the crime . . . . Conspiracy law, however, attacks inchoate crime at a far more incipient stage—the crime of conspiracy is complete at the time of the agreement or (in some jurisdictions) at the time of the first overt act in pursuance of the conspiracy by any party thereto.

WAYNE R. LAFAVE & AUSTIN W. SCOTT, JR., CRIMINAL LAW § 6.4(c), at 530 (2d ed. 1986).

[120] In some circumstances, the security of communication offered by computers may facilitate conspiracy. If, on balance, computers did not increase criminal activity but simply increased the number of conspirators (a possibility that almost certainly would never come to pass) then it would convert this negative aspect of computer crime into a positive one.

employ sketch artists, and build DNA laboratories. This is not so in cyberspace.

Cyberspace facilitates the commission of crimes by permitting users to masquerade as other individuals or as an unknown entity.[121] This enables, and at times exacerbates, all the crimes discussed in Part I. Indeed, the February DDOS attacks would not have been possible without pseudonymity.[122] Of course, in realspace, pay telephones, cell phones, and regular mail offer users some degree of anonymity, but these methods provide mostly point-to-point communications between sender and recipient.[123] On the internet, however, one person can reach millions with a single message.

Encryption is the use of algorithms and other devices to encode data so that it is unintelligible to users who lack the password or key to decipher it. While encryption predates computers by thousands of years,[124] computers have for the first time put encryption into broad use. If you have ever written a document on WordPerfect and "password protected" it, you have used a fairly powerful encryption program. Encryption, obviously, can be used for much more nefarious ends than simply coding a law review article. Ramzi Yousef, who masterminded the World Trade Center bombing, used encryption to store, on his laptop, detailed plans to destroy United States airliners.[125] And many other terrorist networks, such as HAMAS, the Abu Nidal organization, and Osama bin Laden's al Qa'ida, are using encryption as well.[126] Encryption has the potential to threaten effective investigation and prosecution substantially.[127] Accordingly, law enforcement has been worried about the rise of

---

[121] *See Cyber Threats and the U.S. Economy: Hearing Before the J. Econ. Comm.*, 106th Cong. (2000) (statement of Dr. Fred Cohen, Principal Member of Technical Staff, Sandia National Laboratory), 2000 WL 220592 [hereinafter *Cyberthreats*, Cohen] ("[Although creators of digital anonymizers] claim this is to assure personal privacy, my experience tells me that it is used primarily to conceal criminal activities . . . ."); *see also* Rasch, *supra* note 18, at 143.

[122] *Cyberthreats*, Cohen, *supra* note 121 ("[T]he recent denial of service attacks could have been defeated if it weren't for the ease of anonymity in the Internet.").

[123] Charney & Alexander, *supra* note 17, at 943.

[124] 16 NEW ENCYCLOPEDIA BRITANNICA *Cryptology*, at 870 (1990) (stating that Spartans used encryption to issue military commands as early as 400 B.C.).

[125] *Cyberattack*, Vatis, *supra* note 25.

[126] *Id.*

[127] *See Cybercrime Hearing*, *supra* note 21, at 22 (statement of Louis J. Freeh, Director, Federal Bureau of Investigation) ("We are finding more and more . . . computer media as well as stored data, where encryption has made the information and the potential evidence all but worthless or unavailable . . . .").

these technologies, and has offered, unsuccessfully, various proposals to deal with it. One proposal, called the "Clipper Chip," would require computer manufacturers to provide a backdoor entry that would permit the police to read material stored on a computer. Another proposal would outlaw encryption methods that law enforcement cannot decipher.[128]

The problem with these approaches is that encryption is often a good thing. It lets people communicate securely, without fear of interception by curious agents; secret communication often has social value (just think of trade secrets, information from police informants, and romantic messages). Encryption can thus prevent some forms of cybercrime by preserving the confidentiality of data. It also permits remote data networks to flourish and increases the level of trust on the internet by permitting users to verify their identity.[129] An individual can use encryption to create a "digital signature" that is unique to that user, assuring other individuals that a particular data stream is coming from that user (and not an imposter).[130]

This makes encryption, in Larry Lessig's useful phrase, Janus-faced.[131] "Cryptography 'surely is the best of technologies and the worst of technologies. It will stop crimes and it will create new crimes. It will undermine dictatorships, and it will drive them to new excesses. It will make us all anonymous, and it will track our every transaction.'"[132] Given this heaven-and-hell combination, it is easy to understand why the U.S. government has had such a difficult time trying to develop a workable proposal to address the issue.

Pseudonymity raises the same difficulties. Pseudonymity not only provides refuge for criminals, it also provides a host of benefits to legitimate users—benefits recognized by the Supreme Court forty years ago.[133] Political dissidents use pseudonymity to criticize

---

[128] The ill-fated attempts by the Clinton Administration to deal with the encryption issue are beyond the scope of this Article. Interested readers should consult A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995), and Edward J. Radlo, *U.S. Encryption Export Regulations Enter the Twenty-First Century*, COMPUTER LAW., June 2000, at 31.

[129] *See Cyberattack*, Leahy, *supra* note 20 ("Encryption is an important tool in our arsenal to protect the security of our computer information and networks.").

[130] *Cybercrime Hearing*, *supra* note 21, at 64 (statement of Jeff B. Richards, Internet Alliance).

[131] LESSIG, *supra* note 4, at 36.

[132] *Id.* (quoting STEWART A. BAKER & PAUL R. HURST, THE LIMITS OF TRUST: CRYPTOGRAPHY, GOVERNMENTS, AND ELECTRONIC COMMERCE, at xv (1998)).

[133] *See* Talley v. California, 362 U.S. 60, 65 (1960) ("It is plain that anonymity has sometimes been assumed for the most constructive purposes."); *see also* McIntyre v.

oppressive regimes; even our Founders used the pseudonym "Publius" in writing *The Federalist.* People may want to find out about embarrassing products or obtain health information without fear that their identities will be disclosed. Survivors of incest and child abuse may want to meet electronically without fear that their identities will become known. As Jerry Kang has suggested, pseudonymity may be used to allow people to pose as having different genders or racial identities and contribute to broader racial understanding.[134] And these are just a few examples.[135]

The challenge for law is to develop a mechanism that permits the good uses of encryption and pseudonymity to flourish, while simultaneously discouraging the bad ones. Even if the brunt of the current usage of such technologies is negative,[136] government should act with enough foresight to prevent crippling a technology that may ultimately prove useful. This *dual-use problem* is a general one in criminal law. The problem arises when broad categories of action are neither inherently bad nor inherently good. Tension exists between the law's desire to prohibit bad acts and its need to encourage positive applications. In such a circumstance, the law should look not to the act itself, but rather to the context surrounding that act.

Ordinary criminal law, however, tends to conceive of criminal regulations as a binary choice: it punishes acts thought to be inherently bad, such as the taking of human life, and ignores those

---

Ohio Elections Comm'n, 514 U.S. 334, 357 (1995) ("Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights." (citations omitted)).

[134] Jerry Kang, *Cyber-Race,* 113 HARV. L. REV. 1130, 1147 (2000).

[135] Stung from its encryption defeats, and recognizing the push-and-pull nature of pseudonymity, the Clinton Administration shied away from any policy proposals regarding digital pseudonymity. The Justice Department simply acknowledged that pseudonymity can help criminals commit bad acts, but that there are often needs for pseudonymity. DOJ REPORT, *supra* note 5, at 33.

[136] *See, e.g., Cyberthreats,* Cohen, supra note 121 ("[T]he ability to act with relative anonymity in the internet is primarily being used for criminals to avoid attribution and to hide their crimes."). Sometimes negative applications of a dual-use act will undermine its positive applications. For example, pseudonymity can be welcome because it allows people a forum to express themselves without sanction. Once pseudonymity is used to target and attack people, however, those benefits of pseudonymity are destroyed. When I was in law school, and someone pseudonymously started viciously attacking other students in a bulletin board in cyberspace reserved for class discussion, the free-ranging discussion that took place on the board—a discussion enabled in part by pseudonymity—dried up. The account is detailed in LESSIG, *supra* note 4, at 78-82. The lesson may be that government and private actors may need to encroach on a right in cyberspace to allow that particular right to flourish.

thought to be inherently good, such as sheltering the poor.[137] But the "inherent nature" of an act, on closer examination, often turns out to be context-dependent. There are situations in which it is appropriate to take life (for example, in times of war), and times when it is not appropriate to shelter the poor (for example, if the poor person is a felon). Criminal law responds to the problem of "inherently bad" acts that are good in limited contexts by carving out tiny exceptions.[138] These exceptions fall into two categories, call them "licensing" and "proven excuse." Licensing is an ex ante, government-granted exception to a general prohibition, for example, the government's implicit permission for an investigator to carry drugs to bait someone into making a deal.[139] Proven excuse, in contrast, is an ex post exception; it excuses a particular form of conduct only after it takes place. Self-defense is an example. While murder is illegal, murder that afterwards is proven to be in self-defense is permissible.

In general, a license works best when a prohibition would be read too broadly and chill favorable conduct. Licenses are granted as a result of an application process, which may reveal important information about the applicant, allow tracking and monitoring of applicants, provide a suspect list if a crime occurs, and educate the applicant as to the law and its purpose (and as to crime and its harms). In addition, a licensing scheme can penalize those who

---

[137] There is a further modification which incorporates complementarity. If a given act is neutral, but is complementary to an act that is bad, it may be appropriate to punish the given act to avoid incidences of the bad one. This is particularly the case when it is easier for law to detect and punish the neutral act than the other, bad one. *Supra* text accompanying notes 93-95.

There is also a flipside to this complementarity account of bad acts. A given bad act may have, as a complement, a good one. If so, law may not want to punish the bad one because complementarity results in greater utility. If it could be shown that the majority of intruders onto phone company networks cause little harm and actually wind up becoming productive security consultants for the government and industry, for example, law may not want to punish simple unauthorized access because the activity generates net utility.

[138] For acts that are inherently good, the law does not generally intervene. Intervention would be too frequent in such circumstances (James Madison once stated that "[s]ome degree of abuse is inseparable from the proper use of every thing," 4 JONATHAN ELLIOT, THE DEBATES IN THE SEVERAL STATE CONVENTIONS, ON THE ADOPTION OF THE FEDERAL CONSTITUTION, AS RECOMMENDED BY THE GENERAL CONVENTION AT PHILADELPHIA, IN 1787, at 571 (William S. Hein & Co. 2d ed. 1996) (1891)), and it could be a disincentive to commit good acts.

[139] *See, e.g.*, United States v. Singleton, 165 F.3d 1297, 1302 (10th Cir. 1999) (en banc) (holding that anti-gravity statute does not prohibit the government from reducing a defendant's charge in exchange for cooperation: "we simply believe this particular statute does not exist for the government").

engage in conduct without a license, creating a separate crime that can be used as a springboard for investigation, including search and interrogation, into other problematic acts.[140]

Consider one licensing scheme—gun permits. A permit allows the government to force disclosure of whether an applicant previously committed a crime, or has other evidence of instability.[141] If a murder takes place in a particular neighborhood, the police can examine gun registry lists in that location to generate a list of potential suspects. When a gun is bought, the government may require applicants to attend a gun education program. Finally, when government is unable to prove that a particular person committed a specific crime, it may use a gun licensing infraction to search her premises for evidence of the crime and apply leverage to obtain other valuable information from her by offering a plea to the licensing infraction, thus learning about her whereabouts and alibis or, possibly, about accomplices.

Returning to encryption, the government could require a license before an individual uses cryptography. Such licenses could be relatively pro forma, like drivers' licenses, but they would require an individual to certify that these technologies would not be used to further a violation of the law. A violation could result in the loss of the license, a fine, or jail time. Such a scheme carries similar advantages to those regarding guns. First, it would permit the government to garner information about the applicant. Second, licensing would create a list of possible suspects who use a particular encryption algorithm (the mechanism police use to track .22 caliber gunshots might be adaptable to PGP and other cryptography programs). Third, licensing would require individuals to take a

---

[140] The licensing regime calls into question Lessig's broad statement that law regulates "through the threat of ex post sanction, while code, in constructing a social world, regulates immediately." Lawrence Lessig, *The Constitution of Code: Limitations on Choice-Based Critiques of Cyberspace Regulation*, 5 COMM. L. CONSPECTUS 181, 184 (1997). The internalization of the law's lessons and its effects on public morality suggest that laws regulate ex ante just as code does. The fact that law can be broken and that an ex post judgment system is necessary to vindicate infractions does not mean that law is only an ex post system of constraint. Code, too, can be broken by hackers and its ex ante effects neutralized. Law has an ex post vindication mechanism that code largely lacks, but that does not mean law's power is confined to ex post circumstances.

[141] While the application forms vary from state to state, they commonly ask whether an applicant has been convicted of a crime, whether she is a fugitive from justice, whether she has a mental illness, and whether she has been convicted of a misdemeanor offense of domestic violence in state or federal court. *See, e.g.*, MECKLENBURG COUNTY (N.C.) SHERIFF'S OFFICE, PISTOL/RIFLE/SHOTGUN PERMIT APPLICATION (2001), *available at* http://www.co.mecklenburg.nc.us/cosheriff/application.htm.

solemn pledge not to engage in criminal activity, thereby reminding people of the seriousness of a contravening act and creating some self-deterrence. Finally, it would place under immediate suspicion those individuals who use the technology without a license. Such suspicion could eventually culminate in a prosecution, or it could be used as a way for law enforcement to obtain information about other forms of criminal activity. While criminals might try to avoid registration, there may be ways to employ third parties, such as software sellers, to aid in enforcement (akin to gun and car dealers today).

Licensing encryption, however, imposes serious transaction costs. As anyone who has registered a car at the Department of Motor Vehicles knows, it would force individuals to go through the painful hassle of obtaining government permission. It would not necessarily require each individual to obtain a license for simple encryption, such as encrypting a credit card number when buying a T-shirt from Gap.com.[142] But it would force individuals who want to communicate with each other in cipher to obtain a license. Some of those individuals, such as political dissenters, may reasonably fear that the government will use its knowledge that a license has been requested to target them illegitimately, infringing on their constitutional rights of speech and free association. Accordingly, there may need to be acoustic separation between those who maintain the roster of licenses and detectives who could target licensees. Separation would avoid punishing those who opt in to the licensing scheme. The drawback is that the separation would minimize the second advantage of licensing, government tracking.

An alternative to licensing is to permit anyone to engage in the conduct except a particular class (or classes) of people. No license would be necessary; the government would simply *specifically exclude* certain individuals from being able to act in a specific way. The federal law that prohibits former felons and others from carrying firearms is one example.[143] Such strategies do not carry the

---

[142] This is because the web sites themselves could apply for encryption licenses on behalf of themselves and their customers for such limited purposes. The number of licenses permitted by the government could be limited, in order to allow it to monitor adequately the legitimate users of encryption. The government might permit the licenses to be sold on the open market (so long as the government receives notice of the new seller's identity), in an attempt to permit the licenses to go to those who value them the most. *Infra* text accompanying notes 173-74 (discussing advantages of market pricing of a good over government price-setting).

[143] Federal law precludes gun possession by felons, fugitives from justice, addicts, those who have been adjudicated mentally ill or committed to a mental hospital, those

educational advantages of licensing, nor do they allow the government to gain information through the application process. However, if the exclusions are popularly known, they may provide third parties with a greater ability to warn law enforcement of infractions. They may also be helpful in circumstances in which individualistic licensing determinations are, or are thought to be, riddled with prejudice or where case-by-case determinations impose large deadweight losses because of their cost.

Licenses and specific exclusions work by targeting particular *people*; a different accommodation can be reached by targeting particular *acts*. Instead of giving specific individuals or classes of individuals an exemption from a broad prohibition, the law might impose various restrictions on the acts themselves. In the remaining portion of this Part, I outline a few forms of criminal regulation and suggest that this typology provides a useful way of thinking about some of the perplexing problems in criminal law today.

Begin by thinking of the most obvious ways government can address a particular activity: it can either create an *outright prohibition* of the act or it can create an *outright legalization* of the act. Cryptography can either be banned, or it can be legalized. Now let us introduce some more complicated forms of regulation. Return to the problem posed by dual-use technology: an outright prohibition cuts too wide a swath, so government must devise alternate mechanisms.

What might they be? One strategy would *prohibit specific uses* by cataloging the harmful uses and specifically banning them (for example, cryptography cannot be used to further terrorism or drug sales). A more general variant of this approach would simply outlaw any use that furthers a crime. Encryption could be punished, for example, when used to aid in the commission of any criminal offense. (This is actually the tactic used by Nevada and Virginia in regulating encryption.[144]) This approach, however, risks negative substitution

---

subject to a court order restraining them from being near an intimate partner, and others. 18 U.S.C. § 922(g) (1994).

[144] Nevada's statute on the unlawful use of encryption forbids a person from willfully us[ing] or attempt[ing] to use encryption, directly or indirectly, to:

(a) Commit, facilitate, further or promote any criminal offense;

(b) Aid, assist or encourage another person to commit any criminal offense;

(c) Conceal the commission of any criminal offense;

(d) Conceal or protect the identity of a person who has committed any criminal offense; or

(e) Delay, hinder or obstruct the administration of the law.

effects and overinclusiveness. Substitution would occur because if the use of encryption to further a federal offense was itself penalized—with a five-year jail term, for example—then fewer criminals might use encryption to further their offenses, but those that do would likely use it to help commit the most serious of offenses. The law would be overinclusive because it is wasteful to impose a five-year jail term for the use of cryptography in committing a minor offense that itself merits little or no jail time. This is why mandatory sentences, such as 18 U.S.C. § 924(c)'s mandatory five-year term for carrying or using a gun to commit a drug offense, are inefficient and create negative substitution effects.[145]

Instead, the law might attempt to deal with this problem by tying the sentence to the underlying crime. This is what a *standard sentencing enhancement* does. It adjusts a criminal sentence upward by some percentage if various features are present. In current law, those features often include the use of a firearm and obstruction of justice. The Sentencing Guidelines state that one's sentence will increase two levels if a firearm was involved in the commission of certain offenses.[146] A two-level increase in one's sentence is equivalent to about a thirty percent increase in the term of imprisonment. (Sentences double for every six-level increase.)

A similar system of sentencing enhancements could be used to regulate encryption or pseudonymity. That is, one's sentence for a particular crime could increase by a specified percentage if encryption or pseudonymity was used to facilitate the crime. Many courts have described various enhancements as motivated by a desire to increase deterrence, and a new paper by Professors Kessler and Levitt provide

---

NEV. REV. STAT. ANN. § 205.486 (Michie Supp. 1999). Virginia's statute states, "Any person who willfully uses encryption to further any criminal activity shall be guilty of an offense which is separate and distinct from the predicate criminal activity and punishable as a Class 1 misdemeanor." VA. CODE ANN. § 18.2-152.15 (Michie Supp. 2000).

[145] *See* 18 U.S.C. § 924(c) (1994).

[146] The use or presence of a firearm is probably the specific offense characteristic enhancement most sprinkled throughout the Guidelines. U.S. SENTENCING GUIDELINES MANUAL (1998). For instance, a nonexhaustive list of the crimes for which a firearm will enhance the sentence include: aggravated assault, § 2A2.2, minor assault, § 2A2.3, obstructing or impeding officers, § 2A2.4, kidnapping, abduction, or unlawful restraint, § 2A4.1, burglary of a residence or a structure other than a residence, § 2B2.1, trespass, § 2B2.3, robbery, § 2B3.1, extortion by force or threat of injury or serious damage, § 2B3.2, and offenses involving counterfeit bearer obligations of the United States, § 2B5.1.

empirical support for this proposition.[147] For example, the Sentencing Guidelines currently enhance a sentence by two levels when the possession of child pornography "resulted from the defendant's use of a computer."[148] As the Ninth Circuit explained, because "it is difficult to detect and prevent this traffic in cyberspace," the enhancement provision "provides an extra deterrent to those inclined to pursue illicit pictures in the anonymity of the computer world."[149]

Suppose, however, that this regime was not satisfactory to law enforcement because the police could never crack encryption algorithms. Prosecutors would never be able to prove that a criminal used encryption to further the criminal scheme; they would only have a meaningless string of data bits and a defendant clinging to the Fifth Amendment. Then, should this be an endemic feature of a standard sentencing enhancement, the government might levy an enhancement on *particular people, not particular acts.* The government could increase the sentence for anyone convicted of a criminal offense who is found to have used encryption. A defense to the enhancement could be permitted if the defendant can prove that the encryption did not aid in the commission of the offense, thus legislatively flipping the burden of proof for the enhancement and placing it on the defendant.[150] The prosecution need only prove that the defendant used encryption technology. Such an approach may be justified by the difficulties involved in piercing the encryption code.

---

[147] *See* Kessler & Levitt, *supra* note 98, at 358-60 (finding, based on an empirical study, that California's sentencing enhancements produced deterrence); *see also* United States v. Strange, 102 F.3d 356, 361 (8th Cir. 1996) ("While . . . this [enhancement] could, in some cases, result in what might appear to be disproportionate sentences, it is certainly within the province of Congress to resolve that there is some deterrent value in exposing a drug trafficker to liability for the full consequences, . . . of his own unlawful behavior."); United States v. Lewis, 93 F.3d 1075, 1080-81 (2d Cir. 1996) (stating that deterrence is the "animating policy" behind enhancements for crimes committed with "sophisticated means"); United States v. Obi, 947 F.2d 1031, 1032 (2d Cir. 1991) (per curiam) ("Congress, for purposes of deterrence, intended that narcotics violators run the risk of sentencing enhancements concerning other circumstances surrounding the crime.").

[148] U.S. SENTENCING GUIDELINES MANUAL § 2G2.4(b)(3) (1998).

[149] United States v. Fellow, 157 F.3d 1197, 1202 (9th Cir. 1998).

[150] Put slightly differently, the law could be written to place a penalty default on criminals who do not decrypt their transmissions. *See* Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L.J. 87, 97-100 (1989) (discussing the enhancement of social welfare through penalty defaults, which encourage the production of information). This is a standard mechanism that the legislature can use in other areas to avoid difficulties created by the self-incrimination privilege.

The following chart recapitulates much of what has been stated above (though a few items remain to be explained):

NAME	DESCRIPTION	EXAMPLE
1. Outright Prohibition	Penalizes an act, regardless of particular use	"The use of encryption is forbidden, and punished by up to five years in jail."
2. Prohibition of Specific Uses	Penalizes an act if it is done to further underlying criminal activity	"The use of encryption to further any criminal act (defined elsewhere in the code) is forbidden, and punished by up to five years in jail."
3. Sentencing Enhancement for Particular Persons	Enhances a sentence for those convicted of any prior offense if that person committed a particular act (even though that particular act is not itself a crime)	"The prior use of encryption by someone convicted of a federal offense will double a sentence, unless the defendant proves the cryptography did not further any criminal offense."
4. Standard Sentencing Enhancement	Enhances a sentence for those convicted of any offense if the particular act was used to further that offense	"The prior use of encryption by someone convicted of a federal offense will double a sentence, if the cryptography is used to further that particular offense."
5. Licensing	Permits only licensed users to engage in the act; criminalizes use by unlicensed individuals	"To use encryption, an individual must apply for, and receive, a license from the government. The unlicensed use of encryption is a felony."
6. Specific Exclusions	Permits anyone to engage in an act except those specifically excluded	"Anyone may use encryption except those convicted of a previous felony."
7. Detraction for Particular Good Act	Provides downward departure in any criminal sentence if an individual is found to have committed a specified act	"A defendant may receive a one-level downward departure for the use of encryption, when accompanied by no harmful use of encryption, in sentencing for any crime."
8. Detraction for Information	Provides downward departure in a criminal sentence if the criminal provides information that helps government prevent future bad acts or provides information helpful to prosecuting a criminal case	"A defendant who provides substantial assistance to the government in breaking encryption algorithms may receive roughly a 30% reduction in his sentence."

In today's legal debates, academics and policymakers generally draw comparisons between outright prohibition and a few other, less extreme variants of regulation. No systematic attention is given to the role of sentencing enhancements. This is unfortunate, for neither the government nor academics have realized that sentencing enhancements can be a powerful way for the criminal code to achieve a balance between competing aims.[151] Consideration of civil suits and other pricing mechanisms will be deferred until the next Part, though these strategies will promote deterrence as well.[152]

When deciding among the array of criminal options, government must determine whether all instances of an act need to be punished. In making this determination, a key inquiry revolves around whether or not government and individuals can distinguish between positive or benign (A_b) and negative (A_n) uses of the given act. If government can structure a prohibition that only targets A_n, then it should do so. An example is sexual intercourse, which is not targeted when it is consensual, but is prohibited as rape when it is not. But there are two reasons why this solution will not always be readily available. The first occurs when informational asymmetries make it difficult for the law to

---

[151] Even the Sentencing Commission, when drafting the Guidelines, gave little thought to the appropriate use of enhancements. For inside accounts of the process, see Stephen Breyer, *The Federal Sentencing Guidelines and the Key Compromises Upon Which They Rest*, 17 HOFSTRA L. REV. 1, 8 (1988), and Ilene H. Nagel, *Supreme Court Review: Foreword: Structuring Sentencing Discretion: The New Federal Sentencing Guidelines*, 80 J. CRIM. L. & CRIMINOLOGY 883, 923 (1990).

[152] As applied to offenders, criminal regulations are better at shaping tastes than are civil ones, and criminal regulations have the added benefits of avoiding problems with judgment-proof defendants. *See* Katyal, *supra* note 10, at 2442-47 (noting that criminal law focuses less on constraining opportunities and more on minimizing the desire to commit crimes). Due to the several disincentives to bringing civil suits, criminal liability is more likely to deter wrongdoing in cyberspace. *See* Ian C. Ballon, *Pinning the Blame in Cyberspace: Towards a Coherent Theory for Imposing Vicarious Copyright, Trademark and Tort Liability for Conduct Occurring over the Internet*, 18 HASTINGS COMM. & ENT. L.J. 729, 734 (1996) ("Internet tortfeasors and infringers thus are likely to include a high percentage of students and others who may not have the resources to satisfy large judgments."); Pamela Samuelson, *Can Hackers Be Sued for Damages Caused By Computer Viruses?*, *in* COMPUTERS UNDER ATTACK, *supra* note 55, at 479, 484 (acknowledging difficulty with criminal law, but stating that "criminal prosecution is likely to be a more powerful legal deterrent to a hacker than a civil suit is"). This is particularly so for pseudonymity and encryption, which are technologies that make it difficult, if not impossible, for victims to sue those who cause harm. More generally, the existence of judgment-proof defendants may provide an adequate explanation for the use of criminal sanctions. If poorer defendants are placed in jail for their crimes, a distributional equity problem arises if relatively wealthier people can pay to avoid jail. Imprisonment not only answers the judgment-proof defendant problem but also reduces distributional equity concerns.

distinguish between positive and negative variants of the act in a given instance. For example, it may be too difficult to prosecute someone using cryptography because the messages are too difficult for investigators to decrypt; prosecutors would not be able to prove a given message is a harmful A_n instead of a benign A_b. Strategy number one, outright prohibition, may be the best way to prevent harm (though the strategy discussed a moment ago, which reverses the burden of proof, may work here as well).

The second reason concerns informational gaps between the public and law enforcement. If individuals do not know whether a given act falls on the positive or negative side of the line, then they may be deterred from pursuing it. This is a classic problem in the free speech context, but it applies elsewhere in law as well. In other words, self-enforcement will convert a prohibition on A_n into a general prohibition on $A_n + A_b$. Such self-enforcement does not require the government to rule out prohibition. But it does mean that government must investigate what other options can be combined with a prohibition on A_n to redress government's interference in the market.[153]

Again, consider encryption. If its dangers are sufficiently strong, then the government must decide between prohibiting encryption outright, and, more narrowly, prohibiting the use of encryption only when encryption is furthering some criminal act. In making this decision, the points above raise two questions: (1) Is an outright prohibition necessary because the government will not be able to prove that a given use falls on the A_n side of the ledger (that is, that it constitutes a use that furthered a criminal act)? (2) Will a prohibition on A_n be understood by the public as a prohibition on A_b and thereby

---

[153] Some may think a third reason arises from concealment. If a given technology allows near-perfect concealment of criminals, many would clamor for an outright prohibition. If the technology is this powerful, however, of what use is an additional penalty? The government should be indifferent between punishing A_n or $A_n + A_b$, as neither would permit the government to get its hands on criminals given the perfection in the technology. There is one thing, however, that an outright ban does that the targeted approach of strategy number two does not: It greatly diminishes the existence of the lawful encryption industry. In so doing, it makes it more difficult for users to find the technology and much easier for law enforcement to keep pace with stronger variants of the technology. (In the international digital age, however, individuals in other countries may seek to develop and transfer the technology to criminals who will in turn use it for attacks in the United States.) To the extent that the existence of the technology itself shapes tastes towards its use, minimizing its overt appearance on the net may make law enforcement's job easier as well. The case for an outright prohibition, therefore, is that it will retard its ubiquity and technical development vis-à-vis law enforcement's countermeasures.

chill legitimate use of the technology?

If the government has the expertise and technology to prove that specific criminals have used encryption to further criminal offenses, this will militate in favor of using a standard enhancement instead of an outright ban. We will examine the question of when to use such enhancements in a moment. Concentrate now on the second question, for if chilling effects are a serious problem, then government action to correct the skew may be necessary. The government may use four forms of corrections. The first, and most obvious, is to subsidize the legitimate use of encryption.[154] A second way that criminal law may deal with the problem is to heighten the intent requirement necessary to convict someone for the harmful use of encryption. The problem with this modification is that it may be difficult for prosecutors ever to prove that someone specifically intended to use encryption to further a criminal offense.[155]

The third and fourth forms of government action to correct the skew are more subtle, and arise once the civil/criminal patchwork is combined. The third alternative is to permit reduction of a criminal's sentence—for any crime—through a downward departure if the criminal is found to be using encryption only for legitimate purposes (strategy number seven).[156] The last alternative is for the government to permit a downward departure if the criminal provides information that is useful to the government (strategy number eight). If private individuals provide assistance to law enforcement in breaking different forms of encryption software, for example, the government would reward those individuals with a reduction in their criminal sentences. Such rewards can be given to informants in cash or through other means, but giving rewards in the form of downward departures in sentencing sometimes is more effective for a variety of reasons.[157] In many cyberspace prosecutions, the defendant possesses

---

[154] For example, the Internet Tax Freedom Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681-2719, provides that taxes on internet access will not be levied for three years, but the exemption is only applicable to ISPs that offer customers filtering software to limit access to material that parents find harmful to minors.

[155] No witnesses may exist, and intent may be very difficult to divine from a cold computer record. This fact led Congress to water down the intent requirement in the computer crimes statute. *See supra* note 83.

[156] This strategy, however, has the difficult problem of rewarding serious criminals more than less serious ones or innocents.

[157] Social stigma against defection may be lower, the threat of retaliation may be reduced since the criminal will likely face jail time anyway, and a defendant may value a reduction in jail time much more than he values a given amount of money. *Cf.* Michael Lee et al., Comment, *Electronic Commerce, Hackers, and the Search for Legitimacy:*

information that can help government detect and prevent further crimes; criminal law might adapt to this world by creating generalized downward departures.[158] Such departures are a way to harvest valuable information from criminal defendants and promote deterrence through architecture and cost.

Now we return to the complicated question of when to use sentencing enhancements. As noted above, sentencing enhancements are a useful bridge device when a given act has both positive and negative consequences. The Sentencing Guidelines, for example, currently have an enhancement for being a leader.[159] Being a leader, however, is generally a good thing in society and is thus an example of the dual-use problem. Being a leader is only a problem when one is the leader of a criminal enterprise or other nefarious group. Thus the law does not attempt to prohibit leadership; instead it uses a standard sentencing enhancement to increase punishments for those leaders who manage a criminal enterprise. This permits legitimate leadership to thrive and targets only the type of leadership that poses a criminal threat.

Contrast the law's treatment of leadership with its outright prohibition of murder. The dual-use lesson is that whenever law prohibits an act, it must recognize that the act may have positive

---

A Regulatory Proposal, 14 BERKELEY TECH. L.J. 839, 883 (1999) ("Existing literature indicates that many within the hacking community would be willing to cooperate with companies and government agencies if monetary rewards and public recognition were offered for their skills and knowledge." (citation omitted)).

[158] One cost of such departures is that they encourage people to obtain information that might one day be put to harmful uses, such as information regarding the inner workings of a bank's firewalls. Because incentives already exist for people to obtain this type of information (say, because of the monetary benefits that accrue to those who can break a bank's firewalls), the law might consider such departures nonetheless.

[159] U.S. SENTENCING GUIDELINES MANUAL § 3B1.1(a) (1998) (enhancing a sentence for any criminal who was an "organizer or leader of a criminal activity that involved five or more participants or was otherwise extensive").

Two provisions in the existing Guidelines can be used to enhance sentences for computer crime. Section 3B1.3 enhances a sentence for use of a "special skill" in committing or concealing the offense. *See* United States v. Petersen, 98 F.3d 502, 506-07 (9th Cir. 1996) (holding that the computer abilities of a defendant convicted of computer fraud and other offenses supported the special skill adjustment despite the defendant's lack of formal training or licensing). In addition, a common specific offender characteristic is if the offense involved "more than minimal planning." *See, e.g.*, § 2F1.1(2)(A) ("Fraud and Deceit"); United States v. Palinkas, 938 F.2d 456, 462 (4th Cir. 1991) (applying enhancement because defendant was involved not only in the creation of dummy supplier and buyer corporations but also in the development of highly complex computer programs to conceal fraud).

consequences—thus the self-defense exception.[160] The related substitution/marginal deterrence lesson is that law must recognize that there are more and less harmful ways of carrying out that same act. It is no surprise that even with murder, there are greater penalties for those who kill police officers.[161] Permitting the range of the enhancement to be determined by the underlying offense is another way of addressing these problems. Enhancements have the advantage of being pegged to a particular underlying offense so that their penalties can slide with the harm created by those offenses.

The case for the sentencing enhancement for cryptography therefore revolves around three arguments. First, encryption makes it much easier for criminals to thwart law enforcement. Because the expected sanction is a function of the probability of getting caught multiplied by the magnitude of the penalty, a sentencing enhancement corrects the "discount" offered by this new technology. Second, a sentencing enhancement, like strategy number two, which prohibits specific uses, selectively targets specific negative uses of encryption, thus permitting legitimate uses of encryption to continue. Third, a sentencing enhancement slides with the underlying offense, so that the use of encryption to facilitate a bombing is treated much more severely than the use of encryption to sell a marijuana joint. There are certain acts whose disutility is a function of the way in which that act is carried out. The use of 256-bit encryption to further the sale of a joint imposes less harm to society than the use of 256-bit encryption to plan a major terrorist operation.

Law must recognize this variance in harm because penalties should accurately reflect the true disutility imposed by acts and because substitution effects can arise when the law provides inaccurate "discounts" to particular forms of criminal activity. If the penalty on cryptography remains constant whether one uses it to sell one joint or one thousand, people will use cryptography to sell one thousand. This is the problem with Virginia's and Nevada's embrace of strategy number two; by punishing the use of encryption to further criminal offenses, punishment does not slide with the underlying crime and thus creates improper substitution effects.[162]

---

[160] *See supra* text accompanying note 139.

[161] U.S. SENTENCING GUIDELINES MANUAL § 3A1.2 (1998) (providing for three-level, or near fifty percent increase in the sentence). There are also gradations, such as first-degree, second-degree, and manslaughter, but on the whole the law treats murder as an unmitigated evil.

[162] *See supra* note 144.

The Virginia and Nevada statutes could be modified, however, to create separate offenses whose penalties slide with the underlying crimes. In this respect, a strategy that prohibits specific uses can have some of the benefits of a standard sentencing enhancement. Enhancements have an advantage, however, that the former lack: they are easy to understand. The street sign "speeding fines doubled in construction zone" causes me to slow down far more than a sign posting a range of dollar fines. Criminals will find it easier to comprehend the simple command of doubling—for any of the litany of possible crimes—than they would understand the complex schema of sentencing ranges and multiple additional offenses. For example, think of the mental staying power of the "three-strikes-you're-out" laws.[163] (This is why there is a case to be made for such enhancements even if one rejects the wisdom of the Sentencing Guidelines.)

A sentencing enhancement regime is also better suited to rapidly evolving technology. Technology can quickly alter the probability of detection, either positively or negatively. Because Congress is notoriously slow to react to such changes (and often inaccurate when it does react), the Sentencing Commission may be better suited to devising and adjusting optimal penalties in a technologically changing world.[164] There are other advantages to enhancements as well: (1) enhancements may be decided by judges who may have much more technical familiarity as repeat players than do juries;[165] (2) the burden of proof may be lower; and (3) the *Federal Rules of Evidence* do not apply. These advantages may make it easier to determine reliably whether a given use of encryption "furthered" an offense.

Sentencing enhancements have drawbacks as well. Perhaps the most severe occurs when the dual-use activity makes detection by law enforcement difficult. It is important to recognize that this is not an argument that favors prohibition over an enhancement. If

---

[163] Treble damages are easy to understand and remember. It is not surprising that law harnesses them in several contexts. *See, e.g.*, Herbert J. Hovenkamp & Louis B. Schwartz, *Treble Damages and Antitrust Deterrence: A Dialogue*, 18 ANTITRUST L. & ECON. REV. 67, 68, 77 (1986) (outlining the deterrence theory of the treble damages provision in antitrust); Michael J. Metzger, Note, *Treble Damages, Deterrence, and Their Relation to Substantive Law: Ramifications of the Insider Trading Sanctions Act of 1984*, 20 VAL. U. L. REV. 575, 577 (1986) (arguing that Congress passed the treble damages provision in the Insider Trading Sanctions Act of 1984 to maximize deterrence).

[164] *See infra* note 198 and accompanying text (indicating that legislators may be slow to react to changes in technology that alter the probability of detection).

[165] *But see* Apprendi v. New Jersey, 120 S. Ct. 2348, 2363 (2000) (requiring juries to decide certain sentencing departures).

cryptography provides criminals with a foolproof way to avoid being caught, neither an enhancement nor a prohibition will be able to overcome such an advantage. To the extent cryptography provides so many benefits to criminals that no penalty can overcome them, government should develop solutions that emphasize constraints such as architecture and perpetration cost.

Even if encryption provides such overwhelming advantages to a criminal, there may be a limited role for legal sanctions. One way to do so is for law to focus not on bad acts, but on bad persons. This is strategy number three, which *targets bad actors* and imposes a sentencing enhancement on anyone convicted of an offense who engaged in the dual-use act. If Joe is convicted for drug dealing, for example, but is found to have used encryption, he would receive a sentencing enhancement. (This is the inverse of a licensing and specific exclusion regime.) Government could use the strategy to target specific bad actors because such actors are more likely to use the technology for harmful ends.

After all, difficult issues of proof may arise with the use of a standard sentencing enhancement. It may be tough for the government to prove that encryption "furthered" a criminal offense. Indeed, it may be impossible for the government to decrypt any of the message (and it might be inefficient for the government to spend its resources trying to decrypt and prove these things). Furthermore, each time the government seeks such an enhancement, it drains judicial resources. The costs of individualistic determination may be sufficiently great that the government may want to target bad actors instead.[166] The case for strategy number three, therefore, is that government determination imposes large deadweight losses

[166] On the other hand, targeting bad actors risks barring all uses of encryption by certain individuals. To the extent that this technology is one that the government wants to encourage, such a strategy can be very harmful. People may fear that a malicious government prosecutor may target them one day (for perjury, obstruction of justice, or tax evasion) and that their encrypted love letters and legitimate stock transactions might serve as the basis for a sentencing enhancement. It is this fear that animates the standard sentencing enhancement and requires courts to sift through and decide whether encryption furthered a particular offense. Part of the problem can be minimized with burden-shifting strategies that do not criminalize all uses of encryption but place the burden on the defendant to prove that cryptography did not further the offense. This strategy, however, will nevertheless chill more conduct than would an enhancement. This imbalance between preventing criminal communications at the expense of chilling positive conduct may be magnified in circumstances in which the underlying encrypted communication is relevant to a prosecution, but the crime is not serious enough to warrant public exposure of the communication. *See* Wilkes v. Wood, 98 Eng. Rep. 489 (C.P. 1763).

throughout the adjudicatory process *and* that reversing the presumption of encryption as beneficial will require defendants to decrypt their messages. Defendants will be forced to decrypt their communications if government permits a defense to the enhancement for those defendants who prove, perhaps privately to a court-appointed special master, that encryption did not further criminal activity.

Both standard enhancements and enhancements that otherwise target bad actors are motivated by the belief that the government cannot simply target generic acts, like encryption, as illegal. To do so would harm society because of the dual-use problem. Each type of enhancement tries to accommodate this concern by targeting bad people instead of generic acts. The way enhancements define "bad people" differs, but their underlying similarity is the attempt to preserve legitimate uses of the technology without forgoing sanctions on those uses that are harmful to society (through the medium of targeting particular users). But enhancements do not directly incorporate cost deterrence principles. They are really ways of raising law enforcement risks.

How could the legal system promote cost deterrence? In some areas, cost deterrence is quite easy because the government can try to drive up the price of the illegal product. This is a common strategy used with respect to illegal drugs. Because encryption is a dual-use technology, however, a price increase (either through taxation or making such software illegal and creating a black market) has negative repercussions in that it prevents utility-generating applications. A more sophisticated price strategy may be to tax encryption and then rebate the tax to those who certify that they did not commit illegal acts with the technology.[167] In other words, citizens would have to file a pledge under oath that they did not use encryption before they would be eligible for the rebate. The act of signing the statement may generate awareness of the legal risks and may heighten the penalty for using encryption. The upfront tax may also improve cost deterrence by reducing the amount of money that can be invested in criminal activity. This scheme would come closer to targeting bad applications, but it could deter too much lawful encryption (due to high upfront

[167] Section 1441 of the Internal Revenue Code of 1986, for example, requires tax to be withheld on nonresident aliens and foreign corporations. I.R.C. § 1441 (1994 & Supp. IV 1998). The withholding rate may be reduced, however, if the individual or corporation files a certificate with the Internal Revenue Service stating applicability and compliance with specific tax treaties. Treas. Reg. § 1.1441-4(b)(2) (2000).

expenses, complexities of the rebate scheme, etc.).

A different approach to cost might be to use civil forfeiture laws. If individuals engage in criminal activity with the help of encryption, the government could bring a forfeiture proceeding that would seek the computer and all software.[168] Forfeiture laws, however, are not always enforced. Just like legal sanctions, they depend on government prosecutors to bring such cases. Unlike monetary costs, therefore, forfeiture solutions appeal to those criminals who gamble on not getting caught. The probability of forfeiture enforcement may be higher, however, than that for criminal sanctions, as the standard of proof is lower and prosecutors may be more willing to use such mechanisms against low culpability defendants.[169] Indeed, for adolescents who commit computer crimes, forfeiture laws offer much promise as an intermediate solution between imprisonment and letting them go free.

Indeed, there is some evidence that suggests that forfeiture laws are better at deterring criminal activity than threats of imprisonment. A top narcotics prosecutor in Washington, D.C. has stated that, in his experience with nearly 1000 drug cases, the main penalty that successfully deters drug dealers is not imprisonment, but the threat of confiscating dealers' cars.[170] Forfeiture of a computer, following a

---

[168] California provides for forfeiture of a computer, computer system, or computer network, or any software or data residing thereon if it was used in violating the state's computer crimes statute. CAL. PENAL CODE § 502.01 (West Supp. 2001); *see also* N.M. STAT. ANN. § 30-45-7 (Michie 2000) (providing for forfeiture in computer crimes).

[169] *See* Macy v. One Pioneer CD-Rom Changer, 891 P.2d 600, 605 (Okla. Ct. App. 1994) (permitting forfeiture of hardware and software despite Fourth Amendment questions). *But see* Civil Asset Forfeiture Reform Act of 2000, Pub. L. No. 106-185, 114 Stat. 202 (increasing protections against civil forfeiture and adopting a preponderance of evidence standard).

[170] Interview with DeMaurice Smith, Counsel to the United States Attorney for the District of Columbia (Mar. 12, 2000); *see also* Peter Carlson, *Hell's Aged Angel; the Bad Biker Is 61 Now*, WASH. POST, Aug. 9, 2000, at C1 (quoting a former leader of the Hell's Angels gang as stating that one of his three regrets in life was "'losing my right to own a gun'").

Recent research has indicated that California's impoundment laws have had positive results, significantly lowering the incidence of subsequent crashes and traffic convictions for suspended/revoked drivers whose cars were impounded. *See* David J. Deyoung, *An Evaluation of the Specific Deterrent Effects of Vehicle Impoundment on Suspended, Revoked, and Unlicensed Drivers in California*, 31 ACCIDENT ANALYSIS & PREVENTION 45 (1999). Similar results have been reported from other regions. *See, e.g.*, D.J. BEIRNESS ET AL., EVALUATION OF ADMINISTRATIVE LICENSE SUSPENSION AND VEHICLE IMPOUNDMENT PROGRAMS IN MANITOBA 79-82 (1997); R.B. Voas et al., *Temporary Vehicle Impoundment in Ohio*, 30 ACCIDENT ANALYSIS & PREVENTION 635 (1997); Ian Crosby, *Portland's Asset Forfeiture Program: The Effectiveness of Vehicle Seizure in Reducing Rearrest*

conviction for computer crime, may enhance the deterrent and incapacitation effects of criminalization.[171] Furthermore, stripping former felons of their right to use computers for several years following their release from prison can increase cost deterrence and incapacitation even more. New crimes would require additional up-front capital outlays and risk additional legal sanctions. Just as panhandlers may experience a special sense of frustration when their noses are pressed to the glass at Lespinasse, so too may former felons feel a unique discomfort in seeing ubiquitous computers that they may not touch. Computer crime thus would impose not only the cost of jail time, but also the enduring cost of losing one's computer, and perhaps one's economic well-being.

One feature, therefore, of forfeiture is that it dramatically increases the costs for anyone caught once. The first arrest is probabilistic, but after that point, cost deterrence comes into play. To maintain engagement in computer crime, a criminal will need to incur new expenditures, such as buying a new computer and software. These costs may not be dramatic, but they might be enough to deter marginal criminals like teenagers from further criminal activity. Such offenders might have higher elasticities of demand with regard to monetary price than they do with regard to legal risks. When legal risks are also raised through use restrictions, deterrence is further promoted.

We have considered how the government may prevent bad applications of dual-use technology. But how can it encourage good ones? Suppose that the free market will not provide enough of these goods, due to free rider problems, large up-front costs, or other reasons. A host of civil and regulatory measures, such as tax breaks, could spawn these positive applications. I suggest that criminal law, too, can play a modest role in this process, through the use of strategies number seven and number eight.[172]

Among "Problem" Drunk Drivers, http://www.ncjrs.org/policing/port673.htm (1996) (reprinted from POLICING IN CENTRAL AND EASTERN EUROPE: COMPARING FIRSTHAND KNOWLEDGE WITH EXPERIENCE FROM THE WEST (Milan Pagon ed., 1996)).

[171] If legal restrictions could make dangerous software (such as unbreakable encryption and hackers' tools) difficult to obtain, this would increase search costs, as criminals would have to invest more resources in obtaining such software or the skills to program the software themselves. This is a further application of cost deterrence.

[172] In addition, government subsidies might be used to develop countermeasures to criminal conduct. As we shall see shortly, victims and third parties are often in the best position to monitor and prevent criminal activity. *Infra* Part II.B-C. Government may seek to subsidize technologies that permit these actors to carry out their monitoring and thwarting tasks more effectively. If firewalls and anti-virus software are

A powerful line of thought dating back to Hayek explains why the market, not the government, should price goods.[173] According to this argument, the market is best able to determine the true value of a good, whereas the insulated government will inevitably make mistakes because it lacks the proper knowledge about what people need and what they value. Such thinking suggests that the government should stay out of regulating technologies of vast commercial importance. Doing so, the argument goes, poses enormous risks to the formation and accumulation of capital. The view may have some merit, for those setting criminal penalties in the government have no direct stake in these commercial interests.[174] On the other hand, the dangers posed by encryption are so severe that unfettered market control would be far too risky. Again, the law must seek compromise in dual-use situations.

Three potential compromise options suggest themselves: one is conventional; the other two are more novel. The conventional variant is simply to permit government to review the penalty scheme on encryption each year. Congress could be required to hold hearings and industry could lobby and testify for or against the way encryption is being treated. Thinking of law as a dynamic enterprise, in which no penalty need remain constant over the years, gives rise to this possibility. If Congress delegates authority to the more responsive Sentencing Commission, as I have proposed, government might strike reasonable balances between competing aims (given the evolution of technology at different points in time).

The two more novel ways to let individuals help set the price of their conduct involve bidding systems. In the first, individuals could

---

a cheaper way to prevent harm in cyberspace than prosecution, the law might want to rely more heavily on the former and less on the latter.

Some of the approaches outlined above also have the potential to liberate policymakers from raising law enforcement objections to government activity. Suppose, for example, that government decides that encryption should be subsidized because of its important benefits to consumers and companies but resists subsidies due to law enforcement fears. Combining strategy number seven with another approach, such as sentencing enhancements, can remedy the imbalance created by the subsidy and correct the incentives to use encryption for unlawful means.

[173] Friedrich A. Hayek, *The Use of Knowledge in Society*, *in* INDIVIDUALISM AND ECONOMIC ORDER 77, 83-86 (1948) (advocating a decentralized approach to market regulation that leaves decisions to those most familiar with rapidly changing circumstances).

[174] The government of course has a stake in tax revenue, but it is not easy to create a system that forces individual members of Congress or the Sentencing Commission to internalize the cost of this forgone revenue.

bid for the right to have an encryption license. The government could make a case-by-case determination about the money necessary to obtain the license. For example, former felons would have to pay a higher amount than law-abiders. The government would still have the power to decide whether to accept a particular bid, however, and it would still be in the ultimate position to dictate the terms of the exchange. On the downside, this would leave the government open to charges of inefficiency (that the market, not the government, should be responsible for the price) and unfairness (that the government arbitrarily makes some groups or individuals pay more for a license than it does others).

Both of these criticisms could be accommodated by allowing all encryption licenses to be sold on the open market. The market would then price the value of encryption, and the licenses in general would be sold according to a nonarbitrary criterion, that is, sold to the highest bidder. This system, however, forgoes so much government control that it may not succeed. Terrorists such as Osama bin Laden could amass a huge sum of money to buy a license on the open market, while individual mom-and-pops who want the benefits of encryption may be priced out of the market. Given this scenario, we see that there are good reasons to insist on government control of licenses, reasons that hearken back to the enormous danger posed by encryption as well as distributional problems with the allocative mechanism of price.

The other novel alternative is for government to accept criminal, not monetary, bids. To receive a license to use encryption, an individual would bid a specific sentencing enhancement if she is caught using the technology to further a crime. For example, my bid could be 100%, and that bid would signify that if I were caught using encryption to commit a crime, my sentence would double (if I am caught using cryptography to sell five grams of crack cocaine, my sentence would increase from five years to ten). The bid would remind citizens that the use of encryption to further a criminal offense will result in a serious enhancement of their sentence. It would give citizens a stake in the criminal process, one in which they (not the government) are partially responsible for the sentence that they receive. It would permit the government to make flexible determinations based on the conduct of a particular person, allowing the market to suggest, but not control, the ultimate price of the conduct. It would also provide fairness to poorer citizens who want to use encryption but do not have the resources to buy a license from the

government or from an open-market allocative system.

Many will feel that this strategy is too novel. A more palatable bidding system could have individuals bid not on additional jail time, but instead on the degree to which they agree to be monitored by independent, nongovernmental actors. A system could be developed whereby a class of inspectors would periodically examine a user's electronic traffic. The inspectors would not work for the government, and individuals would be free to bid by the name of the inspector as well as the frequency of inspection. This system, once again, would capture many of the advantages of the other bidding systems, such as warning citizens and making them stakeholders, and it may be fairer than a one-size-fits-all approach. In a sense, what I am suggesting is a customer-driven pricing model (Priceline.com meets criminal law) instead of a seller-driven uniform one.

Today's criminal law scholars and policymakers tend to compare a very limited set of options. They examine the benefits and drawbacks of legalization by comparing them to outright prohibition, or perhaps taxation schemes. In their more sophisticated variants, they compare outright prohibition to civil tort suits. But there are many more options, and many more comparisons. These options can be combined in various ways so that the harmful effects of one strategy may be mitigated by embracing another strategy simultaneously.

A return to the pseudonymity debate allows us to sum up. Society should not forfeit the benefits of pseudonymity, but neither can society afford the costs of unfettered pseudonymity. Unfortunately, policymakers have vacillated between these two poles without regard for the options in the middle. In particular, a sentencing enhancement, in either of its varieties, would avoid the disincentive created by an outright ban of pseudonymity and would selectively target its most dangerous forms.[175]

In the early eighteenth century, England made it a capital offense

---

[175] David Post, while recognizing the law enforcement problem created by anonymity, proposes a solution which would legalize pseudonyms. David G. Post, *Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace*, 1996 U. CHI. LEGAL F. 139, 161. Post does not explain what penalties, if any, would accrue to those who use anonymity in communication. Additionally, the use of pseudonymity would have much of the same law enforcement problem, insofar as it would be quite difficult for law enforcement to decode a pseudonym. This problem could be solved by requiring ISPs to maintain lists of realspace identities and accurate decoding sheets, but Post does not suggest any such regime. In any event, an enhancement allows more selective targeting and permits penalties to slide with the severity of the underlying crime.

to poach deer while being "blacked," that is, with one's face covered in disguise.[176] This punishment functioned as a severe sentencing enhancement: simply poaching a deer was subject to a fine of £30 or up to one year in prison, whereas using a disguise to poach meant death.[177] Because deer were so large, they could not be taken quickly unlike smaller animals, so "disguise was the poacher's first protection."[178] Modern-day America similarly should consider increasing penalties when individuals commit computer crimes by stealth, under the cover of pseudonyms, the modern-day equivalent to disguise. The Supreme Court's latest decision on pseudonymity leaves open the possibility for such regulation.[179] Enhancements, in areas such as pseudonymity and encryption, avoid the blunt edge of prohibition by isolating the particular conduct deserving sanction.

c. *Tracing and Escape*

A separate form of reduced costs to the criminal in cyberspace is the ease of escape. Because computer crime can be perpetrated by anyone, even someone who has never set foot near the target, the range of potential suspects is huge.[180] This is unlike traditional crime, in which there is a high likelihood that a crime is committed by someone known to or seen by either the victim or the community in which the crime took place. A criminal in realspace has to be physically present to rob a bank, but a cybercriminal can be across the globe. This makes the crime easier to carry out, easier to conceal, and tougher to prosecute.[181]

Despite some indications of the government's ability to trace criminal suspects online,[182] the truth is that tracing is very difficult. A

---

[176] The Black Act, 1723, 9 Geo., c. 22 (Eng.), *reprinted in* E.P. THOMPSON, WHIGS AND HUNTERS: THE ORIGIN OF THE BLACK ACT app. 1, at 270-71 (1975).

[177] THOMPSON, *supra* note 176, at 58-60. According to Thompson, the Act was motivated primarily by class disputes. *Id.* at 190-97.

[178] *Id.* at 57.

[179] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995); *see also id.* at 358 (Ginsburg, J., concurring) ("We do not thereby hold that the State may not in other, larger circumstances require the speaker to disclose its interest by disclosing its identity.").

[180] DOJ REPORT, *supra* note 5, at 20; ICOVE ET AL., *supra* note 47, at 118; *see* Rasch, *supra* note 18, at 143-44.

[181] Michael Gemignani, *Viruses and Criminal Law, in* COMPUTERS UNDER ATTACK, *supra* note 55, at 489, 492.

[182] *See Internet Denial of Service Attacks and the Federal Response: Joint Hearing Before the Crime Subcomm. of the House Judiciary Comm. and the Criminal Justice Oversight Subcomm. of the S. Judiciary Comm.*, 106th Cong. (2000) (statement of James X. Dempsey, Senior

criminal may leave behind a trail of electronic footprints, but the footprints often end with a pseudonymous e-mail address from an ISP that possesses no subscriber information. Moreover, finding the footprints is often very difficult. Criminals can be sophisticated at weaving their footprints through computers based in several countries, which makes getting permission for real-time tracing very difficult.[183] Unlike a criminal who needs to escape down a particular road, a criminal in cyberspace could be on any road, and these roads are not linked together in any meaningful fashion. The internet works by sending packets of data through whatever electronic pathway it finds most efficient at a given time. The protocol moves these packets a step closer to their destination, an electronic hop, without trying to map out a particular course for the next node to use when the packet arrives. Each hop ends in a host or router, which in turn sends the information on to the next host. What's more, sometimes large packets divide into smaller packets to be reassembled by the end-user when all the packets show up. Sometimes packets never arrive, due to network congestion and mistakes.

So far, I have suggested three problems with online tracing: pseudonymity, weaving through various computer networks, and packet-related problems. There are several additional difficulties. One is that implementing a tracing order is difficult; since the breakup of AT&T, long distance-calls and data transmissions are often handled by several entities. These entities might even be based in other countries, depending on the location of the perpetrator and on whether or not weaving is being used. (The foreign location gives rise to a number of constitutional and statutory questions in each country about whether the transmission can be traced.) By the time the relevant authorities grant their permission, the trail may be cold, as ISPs and other entities may have deleted the information necessary to perform the trace. Furthermore, curious administrators and company officials may damage the trail by poking around.[184] Even if the

---

Staff Counsel, Center for Democracy and Technology), 2000 WL 249419 [hereinafter *Cyberattack*, Dempsey].

[183] *Cybercrime Hearing*, *supra* note 21, at 20 (statement of Louis J. Freeh, Director, Federal Bureau of Investigation).

[184] *Internet Denial of Service Attacks and the Federal Response: Joint Hearing Before the Crime Subcomm. of the House Judiciary Comm. and the Criminal Justice Oversight Subcomm. of the S. Judiciary Comm.*, 106th Cong. (2000) (statement of "Mudge," Vice President of Research and Development, @Stake, Inc.), 2000 WL 232400 ("People implicitly know that they should not wander around a crime scene disturbing potential evidence. Further, when called in to look at a crime scene the investigators will restrict

transmission can be traced quickly before it is damaged, the trace may dead-end into a cell phone line. As cellular phones become commonplace, tracing has become even harder because criminals view cellular phones as "disposable" and treat them like one-time pads to be discarded after use. In addition, the technology to fake cell phone locations and identities is becoming widespread.[185] Even if calls can be traced to a computer in a hard location, there is no guarantee that the user of the computer is present.[186] Effective tracing capability is also hampered by public reaction. Witness the public uproar over Carnivore, and the earlier uproar over the Federal Intrusion Detection Network ("FIDNet"), which would have used intrusion detection software to monitor suspicious behavior on government networks.[187] Fears about privacy therefore also act as a constraint on

---

access .... Unfortunately, it is still the exception when dealing with filesystems and transient data found on computers and networks."), *available at* http://www.house.gov/judiciary/mudg0229.htm.

[185] DOJ REPORT, *supra* note 5, at 28-31. The head of the DOJ's Criminal Division has similarly stated:

> While less sophisticated cybercriminals may leave electronic "fingerprints," more experienced criminals know how to conceal their tracks in cyberspace. With the deployment of "anonymizer" software, it is increasingly difficult and sometimes impossible to trace cybercriminals. At the same time, other services available in some countries, such as pre-paid calling cards, lend themselves to anonymous communications.

James K. Robinson, *Remarks at the International Computer Crime Conference: "Internet as the Scene of Crime"* (May 29-31, 2000), http://www.usdoj.gov/criminal/cybercrime/roboslo.htm.

[186] In the Philippines ILoveYou investigation, for example, police readily traced calls to an apartment in Manila, but the user that launched the virus attack was not apparent. *See* D. Ian Hopper & Reuters Wire Service, *Authorities Seek to Question Pair in "Love Bug" Attack* (May 11, 2000), http://www.cnn.com/2000/ASIANOW/southeast/05/11/iloveyou ("[Authorities] noted, however, that anyone who had access to the apartment and the computer could have created the virus.").

[187] Michael J. O'Neil & James X. Dempsey, *Critical Infrastructure Protection: Threats to Privacy and Other Civil Liberties and Concerns with Government Mandates on Industry*, 12 DEPAUL BUS. L.J. 97, 125-28 (1999).

Fears of Carnivore have been exaggerated. Before Carnivore, if the FBI wanted to tap someone's phone or read her e-mail, it required a court order under Title III, 18 U.S.C. §§ 2510-2522 (1994 & Supp. IV 1998). Carnivore, contrary to press reports, does not change this. All Carnivore does is filter e-mail based on the to and from lines at the top of a message, so that law enforcement can obtain the addressing information and content of e-mails sent by or received by a particular sender provided that a federal judge has given Title III approval. *"Carnivore" and the Fourth Amendment: Hearing Before House Subcomm. on the Const.*, 106th Cong. (2000) (statement of Kevin DiGregory, Deputy Assoc. Attorney Gen., United States Dep't of Justice), 2000 WL 23832328. Rather than the old system of using a human agent to sort through every e-mail (which can pose more severe privacy risks), Carnivore culls addressing information of those messages which are the subject of the Title III judicial order. The

tracing.

The upshot is that it is very difficult for law enforcement to find a criminal after an attack, particularly when the criminal can be on any road and evidence of her crime can be split into numerous subparcels, each of which is not itself incriminating.[188] Even in those cases in which law enforcement has the technology and permission under applicable law to trace an attack, the investigators must be skilled at carrying out such a trace in order for it to be successful, and they must have knowledge about how to preserve the data trails in such a way that they will be admissible evidence in a criminal trial.[189] Regular and frequent training of law enforcement is a necessity, as is up-to-date technological equipment.[190] Government prosecutors and police must also be trained in the application of constitutional and statutory liberties in the internet context.[191] Furthermore, the contraband and materials can be physically stored anywhere on the planet, making such evidence difficult to find and difficult to introduce in a court. Incriminating files of a criminal organization, such as the profits made from drug dealing, may be stored thousands of miles away. Alternatively, the evidence could reside in the United States but be moved abroad literally with a keystroke—whenever a person or an entity comes under criminal suspicion.[192] Computers could also make it easier for criminals to disrupt law enforcement by spying on informants and sabotaging networks.[193]

---

system generates a log of every action it takes, and the FBI only uses it when ISPs do not turn over addressing information. It is basically a souped-up packet sniffer, the kind which private entities have been using for years.

[188] *Cyberthreats*, Cross, *supra* note 54 (describing the complexity of tracing criminal activity over the internet); WILLIAM R. CHESWICK & STEVEN M. BELLOVIN, FIREWALLS AND INTERNET SECURITY: REPELLING THE WILY HACKER 20 (1994) (describing ways in which materials can be delivered regardless of their provenance or address).

[189] DOJ REPORT, *supra* note 5, at 12; STOLL, *supra* note 44, at 109 ("We're accustomed to handling most forms of white-collar crime—we recognize the telltale evidence .... Over the networks, these are impossible without sophisticated tools like digital signatures or cryptographic keys.").

[190] DOJ REPORT, *supra* note 5, at 28-29.

[191] *Cybercrime Hearing*, *supra* note 21, at 60 (testimony of Jeff B. Richards, Executive Director, The Internet Alliance).

[192] DOJ REPORT, *supra* note 5, at 21 ("With scores of Internet-connected countries around the world, the coordination challenges facing law enforcement are tremendous. And any delay in an investigation is critical, as a criminal's trail often ends as soon as he or she disconnects from the Internet."); Wittes, *supra* note 3 (explaining the ease with which large amounts of information can be moved around electronically).

[193] *See* TSUTOMU SHIMOMURA & JOHN MARKOFF, TAKEDOWN 238 (1996) (describing how hacker Kevin Mitnick disrupted law enforcement by changing police

Because these factors lower the probability of successful enforcement, it may be appropriate to offset this lowered probability by increasing the magnitude of the criminal sanction. Doing so would avoid substitution effects and result in balanced sanctions. Some may reject this approach, arguing that computer crimes require a high upfront investment in skills, thereby canceling out the efficiencies of cybercrime. Whatever else may be said, it is highly unlikely that computers—which have produced such complicated phenomena in noncriminal society—would give criminals the exact balance of benefits and costs necessary to moot each other out. The natural desire for simplicity must not blind us to understanding these effects. The upfront investment point, moreover, ignores a key feature of the computer world: software. All that is really necessary for a cybercrime to take place is that someone provides the tools—encoded in a program—to surmount defenses. It is therefore not surprising that programs such as hackers' tools are proliferating on the internet, enabling even those without technical sophistication to commit dangerous crimes.[194]

Cybercrime is thus somewhat different from regular crime in that it initially requires sophistication and expertise, but that sophistication and expertise can be given fully to others who lack it. Even though I do not know how to code a word processing program, I am perfectly happy to use WordPerfect to write this very Article. Similarly, a weak-

---

officers' phone numbers and credit reports). For example, a raid of the Cali cartel headquarters in Columbia found two IBM mainframe computers that cross-checked every phone call to the United States Embassy and Columbian Ministry of Defense against phone books to discover the identities of informants. *See supra* note 51 (describing the mafia's use of computers to disrupt law enforcement).

[194] *Cyberattack*, Vatis, *supra* note 25 ("While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the World Wide Web and launch them against victim sites. Thus while attack tools have become more sophisticated, they have also become easier to use."); *Cyberthreats*, Cross, *supra* note 54 (same).

Many web sites provide information and tutorials about how to commit computer crime. *See, e.g.*, Black Sun Research, *Tutorials*, http://blacksun.box.sk/tutorials.html (last visited Feb. 9, 2001) (teaching novice and more experienced hackers how to hone their hacking skills); Happy Hacker, *You Mean You Can Hack Without Breaking the Law?*, http://www.happyhacker.org (last modified Feb. 8, 2001) (relaying up-to-the-minute hacker news and providing lessons in hacking). Also, anyone can buy programs such as the "Elite Hackers Toolkit," "Hacker's Underworld," and "Master Hacker," all of which contain programs to crack passwords, undermine firewalls, hijack information packets, and launch viruses. I visited a commercial software sales site, Most Significant Bits Corp., *Shop Online for Computer Software, CD-ROM Titles At the Guaranteed Low*, http://www.nothingbutsoftware.com (1997-2000), on October 23, 2000, and found all of these products for sale for prices between $12-$17.

brained cybercriminal does not need to know much about the technology in order to run an executable file. This gives a great deal of power to computer programmers and suggests that the government must treat them differently from program users because of the great potential for programmers to use their techniques to bad ends. It also suggests a further wrinkle in cyberspace regulation: government may need to regulate even innocent software programmers who write material that facilitates crime. The regulation of programmers will pose a much greater problem in the new millennium, as the litigation over Napster demonstrates. Because individual users are dispersed across the country and around the globe, regulating software authors may be necessary to curtail crime on the net. This is particularly so if the widespread availability of hackers' tools and other dangerous software shapes tastes towards crime.[195]

It is possible to envision a world in which the technological, legal, and practical barriers to online tracing eventually dissolve. That world appears far off, given architectural barriers such as disposable cell phones, but it is possible. If tracing reached the point where it was more effective than detection of realspace crimes, the analysis thus far would need to be rethought.[196] Penalties would need to be revised as well, insofar as they were designed for an age in which crimes were tougher to solve. For example, the District of Columbia recently installed cameras to catch those who run red and yellow lights. Now that getting away with running a light is virtually impossible, lots of people are stuck with very large fines for the practice.[197] This is because the high penalties were designed to compensate for the low probability of enforcement. As technology increases that probability, the sentences must adapt.[198] For the present, however, remoteness and invisibility confer large advantages on cybercriminals and legal

---

[195] *See* JON ELSTER, SOUR GRAPES: STUDIES IN THE SUBVERSION OF RATIONALITY 25 (1983); Katyal, *supra* note 10, at 2441-42 ("[W]hat people want may be a product of what they can get.").

[196] At least some of the benefits of tracing may be ones that help solve realspace crimes. *See supra* note 108.

[197] *See* Arthur Santana, *Camera Ready—or Not*, WASH. POST, Apr. 2, 2000, at C1 (describing the effectiveness of the camera system in "catching an average of 41 red-light runners a day"); Arthur Santana, *Seeing Red Over 'Gotcha' Camera*, WASH. POST, May 19, 2000, at A1 (reporting "billing $1.5 million [to red-light runners] in just over six months"); *see also* Sylvia Moreno, *In Alexandria, Fail to Stop and Camera Goes Pop!*, WASH. POST, Nov. 13, 1997, at D1.

[198] Interesting cross-institutional problems arise as legislatures may not be able to act quickly enough to reflect changes in technology (which will often take effect without legislative approval). The result may be serious overdeterrence.

institutions need to address these changes.

I shall return to the theme of distance between criminal and crime later in this paper. Remoteness not only lowers the probability of the enforcement of criminal law, but also largely precludes the use of social norms as a way to constrain deviant behavior and explains why trendy theories of enforcement such as Broken Windows policing need to be adapted to invisible crime on the net. Furthermore, because the enforcement of criminal law, online tracing, is less visible than cops on the beat, the government also faces challenges due to the remoteness of its methods. Before delving into these issues, I shall first examine the role of other parties besides law enforcement in deterring cybercrime.

B. *Second-Party Strategies of Victim Precaution*

1. Optimal Victim Behavior

The existence of cost deterrence suggests that the government should not rely exclusively on sanctions to prevent crime. The government cannot be omniscient and omnipotent, nor would we want it to be. For that reason, other entities must act to make crime more costly; doing so reaches a more efficient result.[199] Examples from realspace include placing locks on doors and not leaving items of value in plain sight. It is far cheaper to have each car built to require a key for entry and use than it is for the government to try to police the illegal entry and use of every vehicle in America. By altering the extent of private protection, law can influence constraints such as perpetration costs and architecture.

For some types of cybercrime, reliance on victim precaution is optimal because the cost of government identification, investigation, and prosecution of the crime is too great. For example, if many computer bugs can be prevented with the use of simple software, such as Symantec Anti-Virus, the software may prevent crime more cheaply than relying on government enforcement of legal sanctions. Indeed, many major crimes, such as MafiaBoy's DDOS attacks, can be prevented with easy-to-use technology and common sense.[200]

---

[199] *See generally* Omri Ben-Shahar & Alon Harel, *Blaming the Victim: Optimal Incentives for Private Precautions Against Crime*, 11 J.L. ECON. & ORG. 434 (1995). At times, government prosecution may be warranted even when a victim did not take precautions because prosecution yields social benefits that exceed its costs, including the cost of diminished precautionary actions.

[200] The Internet Engineering Task Force, as early as January 1998, proposed a very

If the cost of government prosecution is high, it may be appropriate for the government to give priority to prosecuting those cases in which the victim took adequate precautions (or, in extreme cases, refusing to prosecute cases in which victims took no precautions at all). Doing so will provide some incentive for potential victims to take these precautions. And it will conserve government resources, for investigating and prosecuting each of the millions of cybercrimes is financially impossible.[201]

A powerful counterargument emphasizes the limited incentives created by the government for victims to protect themselves.[202] If a victim is cavalier about the data on her computer and does not use anti-virus software, why would the speculative threat of government prosecution matter to her? If the threat of data loss is not enough to encourage a person to take quick and easy precautions, the priorities of prosecutors are not likely to make a difference either. This is a standard problem with blame-the-victim strategies: government prosecution is not valuable enough to a victim to induce the desirable precautionary behavior.

But there is a rejoinder to the argument: the change in incentives is not so much on the part of *victims*, as it is on the part of *police*. Police are currently ex post machines, able to track down criminals and investigate crime scenes. They are not focused on prevention so much as they are on prosecution. This system makes sense in realspace insofar as there is a finite amount of crime that can take place at once, given corporeal constraints. But in cyberspace, where the incidence of crime may be high and the ability to track cybercriminals may be low, government may need to change its

---

simple way to preclude DDOS attacks. *Cyberattack*, Dempsey, *supra* note 182; *see also* William L. Scherlis et al., *Computer Emergency Response*, *in* COMPUTERS UNDER ATTACK, *supra* note 55, at 495, 495-96 (proposing that the common errors of lax password policies and failure to use published fixes for security holes can be easily corrected).

[201] The government already prioritizes computer facilities through its Key Asset Initiative to designate those systems of particular importance to the United States. *Cyberattack*, Vatis, *supra* note 25.

[202] In suggesting a role for prosecutorial priority shifting, I intentionally do not discuss government regulation of victim behavior, though such strategies should be considered as well. Law-abiding entities may be more responsive to regulation compared to computer criminals. However, government may not be sufficiently aware of the cost of such safeguards, and regulation may thus interfere with established market behavior in unpredictable ways. *See infra* Part II.B.2. Using ex post prioritization of cases, by contrast, permits the class of entities who are potential victims to evaluate their own level of risk, as well as the costs and benefits of additional protection. Because prosecutors and police would be able to assess victim precaution against industry-wide custom, it may be more efficient than a priori regulation.

prosecution strategy towards warning potential victims of threats to their computers.[203] The FBI has been quite good at warning computer users about specific attacks once they learn about them, as with the Melissa virus,[204] but has not been particularly concerned with teaching computer users about adequate safeguards ahead of time. Law enforcement needs to think less like traditional police departments and more like fire departments, emphasizing education and appropriate computer hygiene in public outreach campaigns.[205]

Providing warnings is not sexy stuff for police, who would much rather be chasing criminals than giving speeches, and changing their attitudes and inclinations will be quite difficult. A rule that permitted police to open criminal cases only once they knew victims had taken appropriate precaution, however, would help induce this shift in police behavior. By coupling the desirable police activity (chasing criminals) with the less desirable activity (giving warnings), police would have incentives to pursue the latter.[206] The warnings could be educational, in that the police could discuss computer security threats, common ways of preventing them, and the inability to open a criminal case unless victims take certain basic forms of precaution.

Two differences must be considered between realspace and cyberspace at this juncture. First, in realspace crime, the government is reluctant to embrace measures that emphasize the power of victim precaution because they unfairly penalize innocent third parties instead of combating crime. In the computer context, by contrast, there is quite a strong reason to induce victims to engage in preventive measures. The government is unable to police the internet in the same way it is able to police the city streets. Visibility of crime is

---

[203] *See Cyberthreats*, Cross, *supra* note 54 (arguing that information, education, and training are necessary to harden cyber targets and prevent crimes from occurring in the first place); *Cybercrime Hearing*, *supra* note 21, at 63 (statement of Jeff B. Richards, Executive Director, Internet Alliance).

[204] *Cyberattack*, Vatis, *supra* note 25 (discussing how the Melissa Macro Virus was treated under the FBI's two-fold response, "encompassing both warning and investigation—to a virus spreading in the networks," and explaining that "[t]he NIPC sent out warnings as soon as it had solid information on the virus and its effects; these warnings helped alert the public and reduce the potential destructive impact of the virus").

[205] *See Stakeout Press Briefing with Business and Technology Leaders Following Meeting with President Clinton on Internet Security*, FED. NEWS SERVICE, Feb. 15, 2000 (demonstrating that the industry advocates a similar position).

[206] To create the correct incentives, the same police officer should be responsible for the educational campaigns and the investigation of criminal wrongdoing at a particular facility.

low and much of the technical information necessary to forestall an attack and to facilitate investigation of a crime resides only in the hands of private entities.[207] And the vast number of computer attacks—and the potential for them to continue to multiply—suggest that the government may need to change its model.

Governments should, in short, first prosecute those crimes in which the victim engaged in the optimal level of precaution. If resources and energy are left over, then the government should investigate those other cases in which the victim did not take preventive steps. Such a strategy changes the constraints of cost and architecture, making cybercrime more expensive and more difficult to carry out. Note again that these forms of deterrence work even when criminals know nothing about the law and even when they believe there is no chance of getting caught by police.

In order to do this effectively, government cannot simply treat all victims as equal. It is not optimal for Chevy Chase Country Club to take the same preventive measures as Chase Manhattan Bank. Too much money would be spent preventing the crime and deadweight losses would be incurred. To maximize efficiency, government could use a formula that compares the cost of preventing the crime against the potential monetary loss that an intrusion could generate. The famous Learned Hand formula that every first-year torts student learns might be applied in the area of criminal law on the internet.[208]

---

[207] First, most of the victims of cyber crimes are private companies. Therefore, successful investigation and prosecution of cyber crimes depends on private victims reporting incidents to law enforcement and cooperating with the investigators. . . .

. . . .

. . . Second, the network administrator at a victim company or ISP is critical to the success of an investigation. Only that administrator knows the unique configuration of her system, and she typically must work with an investigator to find critical transactional data that will yield evidence of a criminal's activity.

Third, the private sector has the technical expertise that is often critical to resolving an investigation.

Cyberattack, Vatis, *supra* note 25; *see* O'Neil & Dempsey, *supra* note 187, at 103 ("The infrastructures at issue are largely privately owned. Those private owners have a substantial economic stake in protecting their investments . . . . Those who own and operate these systems are in the best position to understand and prioritize this range of threats and what is necessary to mitigate them." (citations omitted)); Robinson, *supra* note 185. In addition, victims must cooperate with the government after an intrusion for effective prosecution. *See* Charney & Alexander, *supra* note 17, at 946 ("[I]t is simply not possible for investigators and prosecutors to become instant experts in every type of system, in light of the wide array of computers and operating systems on the market. . . . [W]e will often need the victim to assist us in our efforts.").

[208] For a description of the test, see *infra* text accompanying notes 223-26.

Government should concentrate its resources and fight those crimes in which victims could be considered nonnegligent. Unlike entrenched areas of law, cybercrime is a new area and government has a unique opportunity to influence the path by which potential victims take precautionary behavior.

Second, the interlinkage of victims in cyberspace makes computer crimes different from realspace ones. In realspace, when one victim visibly self-protects, it does not advance the general welfare tremendously; it simply displaces the crime. (A "Club" placed on a car illustrates the point: it merely keeps that particular car from being stolen.[209]) In cyberspace, by contrast, many forms of victim self-precaution generate positive externalities by increasing the perpetration costs of crime generally.[210] The point is best understood with reference to computer viruses.[211] The ILoveYou virus, for example, infects the root e-mail system and sends the virus to fifty additional people, who in turn pass it on. Each inoculated computer could prevent thousands of additional infections. (The virus analogy is particularly apt. In public health this phenomenon is known as "herd immunity"—the concept that even if my child is not vaccinated, the vaccinations of others will prevent my child from being infected—though, to my knowledge, computer experts have not borrowed the term.)

There are other crimes in cyberspace where victim precaution is

---

[209] *See* Ian Ayres & Steven D. Levitt, *Measuring Positive Externalities from Unobservable Victim Precaution: An Empirical Analysis of Lojack*, 113 Q.J. ECON. 43, 44 (1998) (providing other examples including "visible car alarms [and] home-security systems" and distinguishing unobservable precautions such as Lojack). Many forms of self-protection in cyberspace will be invisible. Those precautions that are visible or otherwise apparent, however, may externalize crime onto those victims who take comparatively less precaution.

[210] There are some realspace analogues, such as merchants on a common neighborhood block who discuss vagrants and suspicious characters or, perhaps, major financial institutions which prepare plans to protect the physical security of their infrastructure. Some cooperative victim precautions, such as common software, nevertheless mean that the same vulnerability can exist in more than one system. In the Cliff Stoll case, for example, a laboratory at Berkeley as well as an Army munitions base in Alabama both ran the same commercial UNIX program, and the loophole in security permitted the East German hackers to run computer programs at both sites, as well as many other computers nationwide. STOLL, *supra* note 48; *see infra* note 271 (discussing the value of diversity in software and hardware).

[211] *Internet Denial of Service Attacks and the Federal Response: Joint Hearing Before the Crime Subcomm. of the House Judiciary Comm. and the Criminal Justice Subcomm. of the S. Judiciary Comm.*, 106th Cong. (2000) (statement of Katherine T. Fithen, Manager, CERT Coordination Center), 2000 WL 249418 [hereinafter *Cyberattack*, Fithen] ("Everyone's security [on the internet] is intertwined.").

socially optimal as well. For example, securing sites against intrusions will prevent hackers from using these sites to attack other sites and mask their trail. DDOS attacks become virtually impossible and the difficulty of weaving one's electronic trail is increased. In sum, there may be some crimes in cyberspace for which victim self-protection is particularly important because it produces positive externalities that advance general welfare. Because the benefits of victim precaution do not inhere only to the victim, government may need to encourage this precaution.

2. The Limits of Victim Precaution

Not all strategies for victim precaution are optimal. Many methods will impose significant losses, and these losses must be considered if the government prioritizes cases on the basis of victim precaution. Indeed, a strong presence by law enforcement in cyberspace is necessary precisely because victim precaution is something to be feared, not welcomed, in many instances.

To understand the point, think about cities in which crime is rampant. People lock their doors, are afraid to venture out in public, and rush their children home from school without speaking to each other. A community cannot flourish under conditions in which trust has broken down. Instead, society atomizes and its residents live in fear. These forms of victim self-protection, from bars on windows to avoiding public spaces, impose substantial losses. And once societal cohesion has broken down in this way, it is difficult for cohesion to return.

The infancy of cyberspace presents the government with a unique opportunity to prevent the net from mirroring our inner cities. Without vigilant government protection and prosecution, two harms may befall the internet. First, the internet could fragment into a series of trusted networks for privileged users.[212] Individual sites, particularly new ones, will not let users access their information without adequate assurance that they will refrain from hacking and stealing private information. Accordingly, site managers will insist on high assurances that a person accessing a site is legitimate and will deny entry to those whose provenance is questionable. Unlike commercial establishments in realspace, web sites need not open their

---

[212] For a description of trusted networks, see Mark Stefik, *Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us To Rethink Digital Publishing*, 12 BERKELEY TECH. L.J. 137, 139-44 (1997).

doors to anyone. The lack of regulation and due process characterize these transactions. The marginal benefit from one extra customer of dubious origin is exceeded by the damage a cyberthief can do to the site. (In realspace, a similar phenomenon occurs, regrettably along racial lines, when stores do not let "questionable" customers shop on their premises.) This can stymie development of the internet and make it difficult to secure the commercial and other advantages the technology promises to provide.[213]

The upshot of an over-reliance on victim precaution may be to return us to the age of the electronic bulletin board. When I was twelve years old, I used my Apple II to dial up various bulletin boards across the country and electronically chat with different users and swap programs. At no time would a board have more than ten people on it, and rarely would any one board have more than a few files of interest. No board was linked to the next one and there was no way of searching the individual boards to know who or what was on the others. With the connectivity of the internet, however, these problems have dissolved. Instead of isolated enclaves, web sites on the internet are linked together in ways that encourage users and programs to work together. The countless hours spent dialing and searching each board seriatim are over. Victim precaution can undermine this trend and force technology to spiral backwards.

Too much reliance on victim precaution will also cause a second phenomenon. Instead of denying access altogether, web sites will build strong firewalls to prevent access to certain areas of their sites.[214] A firewall is like a tollgate. It requires all electronic traffic to request entry by passing through the firewall. Without the proper authorization, however, the firewall blocks traffic by using a filter or "screen." It may also funnel the incoming traffic to designated areas. Further detail is too complicated for our purposes here, what is important is simply to understand that firewalls, properly built, allow

---

[213] Even President Clinton recognized that protection against internet crime is necessary to mine the internet for commercial opportunities. *See* Remarks Prior to a Meeting with Technology Industry Leaders and Computer Security Experts and an Exchange with Reporters, 36 WKLY. COMP. PRES. DOC. 308 (Feb. 15, 2000), *available at* http://www.cdt.org/security/000215whitehouse.shtm.

[214] Alternatively, sites could use intrusion detection systems to monitor their networks and data. The problem is that the systems have so many false positives that users eventually turn them off, and even when the systems are on, the warning typically comes too late in the attack process. For a description of intrusion detection systems and false positives, see Marcus Random, *Intrusion Detection: Ideals, Expectations, and Realities*, 15 COMPUTER SEC. J. 1, 2-3 (1999), *available at* http://www.gocsi.com/intrus.htm.

web sites to block any type of incoming or outgoing traffic they wish.[215] A university that does not want its students to access certain pornographic web sites with university computers can either publish a regulation punishing such conduct or employ a filter to do it for them. A neighborhood bank may be afraid of traffic from Israel because of the high percentage of hackers there and can block all incoming traffic originating in Israel.

Firewalls, however, impose large costs. These costs include: hardware and software purchases, programmer time, hardware maintenance and software upgrades, administrative setup and training, inconveniences and lost business opportunities resulting from a broken gateway or denial of services, and an inevitable loss in connectivity.[216] Such costs vary with the type of firewall selected. For example, packet filters require quite complicated and up-to-date information about ports on the internet. They may slow down the domain name system and recognition of a site by other hosts and make it more difficult for a site to communicate with the outside world.[217] They also slow down local networks considerably, adding to worker frustration and loss of productivity.[218]

Any government inducement for firewalls, whether through shifted prosecutorial strategies, contributory negligence in tort, or taxation incentives, must take into account the variances in costs and benefits that accrue to different users. The costs of firewalls are not trivial. It can be said that the two chief advantages of the internet lie in its ability to provide information rapidly and its potential to connect users who previously were not connected. Both of these advantages are undercut by widespread and strong firewalls.

In economic terms, the internet takes advantage of network effects. A network effect occurs when the utility of a good increases

---

[215] Firewalls come in three general varieties: packet filtering (which denies access to packets based on their source or destination addresses or ports), circuit gateways (which bypass areas of a site that cannot be accessed by outside traffic), and application gateways (which employ filters within each individual application, such as e-mail). An excellent description of the code necessary to build these walls is contained in CHESWICK & BELLOVIN, *supra* note 188, at 85-118. *See also* Tom Sheldon, *General Firewall White Paper* (Nov. 1996), http://www.ntresearch.com/firewall.html.

[216] CHESWICK & BELLOVIN, *supra* note 188, at 51-52. Firewalls also need to be updated to take account of new threats to the firewall as well as ways to exploit bugs in the original program design. *Id.* at 83.

[217] *Id.* at 62-64.

[218] *See id.* at 74 (discussing the "performance penalty for packet filtering").

with the number of other agents who are consuming the same good.[219] The internet's value lies, at least in part, in exploiting these network effects. As more people come online, the value of the internet increases. E-mail, for example, is more valuable to me this year than it was last year because my mother has now learned how to use e-mail. The standard phrase to capture this is "Metcalfe's Law"—that the value of participation on a computer network grows *exponentially* with the size of the network.[220] While this is an exaggeration, the larger the number of people online, in general, the greater the advantages there are.

Certain forms of victim precaution, however, can undermine this trend and create electronic balkanization. An example familiar to even a novice user of the net concerns internet searches. Most of us have conducted searches on sites such as Yahoo! or Google. I can type my name into these engines and find a variety of information about myself—from my college activities to law review articles I have written. For a search engine to work, two levels of access are thus necessary. The search engine itself requires access to individual sites in order to search through and catalog the material, and an individual user requires access to read the material on the site. Both levels require trust between the two parties involved in each transaction. Without trust between the engine and the individual web site, the engine cannot catalog or search through the material.[221] And even when access is granted to the search engine, access may not be granted to the individual user (for example, when Yahoo! brings up a hit on

---

[219] Michael L. Katz & Carl Shapiro, *Network Externalities, Competition, and Compatibility*, 75 AM. ECON. REV. 424, 424 (1985); *see also* Michael L. Katz & Carl Shapiro, *Systems Competition and Network Effects*, J. ECON. PERSP., Spring 1994, at 93, 94 ("Because the value of membership [in a network] to one user is positively affected when another user joins and enlarges the network, such markets are said to exhibit 'network effects,' or 'network externalities.'"); S.J. Liebowitz & Stephen E. Margolis, *Network Externality: An Uncommon Tragedy*, 8 J. ECON. PERSP. 133 (1994) (refining and limiting the Katz & Shapiro concept).

[220] George Gilder, *Metcalfe's Law and Legacy*, FORBES ASAP, Sept. 13, 1993, at 158, 160; *see also* Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CAL. L. REV. 479, 483-84 (1998). In one sense, however, the internet's value decreases with additional users due to the technological limitations of bandwidth. The more users there are on the net, the slower the internet's response time.

[221] Some search engines use Web "spiders" to search automatically through material and catalog it. Individual sites can generally prevent these spiders from entering by altering their "robots.txt" file, but doing so has the cost of reducing the amount of material that can be searched online. Martijn Koster, *A Standard for Robot Exclusion*, http://info.webcrawler.com/mak/projects/robots/norobots.html (last visited Nov. 2, 2000).

certain newspapers, the newspaper may not let the user read the article without registering).[222]

But there is a third layer involved here, and it is this layer that may be the most puzzling: the value of the network can be diminished by too many users. If I want to chat with people about the history of the year 1776, I do not want my chat to involve the one million people online who know something about that year. Similarly, if I want to search the web for information about the year 1776, it is not helpful to retrieve 50,000 hits. People are not computers. They have limited attention spans and weak multitasking capabilities. The value of the internet lies not only in its ability to maintain vast amounts of material and users, but also in its ability to filter and separate the data into an accessible form. For such filtering to take place, trust between the parties is essential. The search engine must have sufficient access to each web site to ensure that its catalog reflects a semi-intelligent understanding of the material; the individual user must let the search engine know enough to conduct a proper search.

Any calculation of optimal victim precaution must therefore take into account the harms imposed by such precaution. It is dangerous to expect victims to do too much. And yet much legal scholarship simply assumes away the problem. Consider torts. The famous Learned Hand Test states that negligence depends on whether the burden of private precautions exceeds that of the probability of an accident multiplied by the harm of that injury.[223] In the case that gave rise to the test, a ship had broken away from its tow and smashed into a tanker.[224] The ship owner sued the towing company, but the towing company said that the ship owner was contributorily negligent for not having an attendant on board.[225] Hand sided with the towing company, stating that the ship owner could have avoided the accident

---

[222] For example, on the day the majority of Verizon Communications workers returned to their jobs, I went to *Yahoo! News*, http://dailynews.yahoo.com/headlines, to read about the strike. I found a link to a magazine article, *The Guilded Rage*, published by the *New York Times Magazine*. When I clicked on the link, I was brought not to the article itself, but to the *New York Times* registration page, http://www.nytimes.com/auth/login?URL=http://www.nytimes.com/library/magazine/home/20000820mag-ethicist.html. Before the *Times* would grant me the privilege of reading their article, they wanted information about me in exchange (including my name, sex, age, household income, zip code, country of residence, and e-mail address).

[223] United States v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947).

[224] *Id.* at 171.

[225] *Id.*

by having placed an attendant on board.[226] Hand, however, trained his eye only on the cost of precautions to the ship owner. While this limited focus may have been appropriate on the facts of that case, the general formula needs revision.

When private precautions impose negative externalities (in that they cause harm that is not borne exclusively by the precautionary party), the Hand test will lead to a suboptimal result. Focusing only on the victim's costs, without due regard for the cost of the precautions to society, can skew reasoning. Computer crime is a nice illustration of the point. If victims build firewalls that are too strong, collective benefits will be undermined. As the Cornell Commission Report on the Morris worm case states, a "community of scholars should not have to build walls as high as the sky to protect a reasonable expectation of privacy, particularly when such walls will equally impede the free flow of information."[227]

The government must therefore encourage the growth of networks by preventing enough crime to stop electronic balkanization. Just as in realspace, the police must provide a level of security that permits people to live their lives on the net and expand their communities. The fear of crime can stifle this human outgrowth. The government cannot force people to trust each other, nor can it force our computer networks to trust each other. The only solution lies in the government eliminating enough intrusion to permit people to feel secure. Any strategies that rely on victim precaution must be tempered by recognition of the value of network effects.

3. The Emergence of a Special Form of Crime: Targeting Networks

This discussion of network effects and computer crime also encourages a partial reconceptualization of what crime is. Traditional criminal law focuses on crimes to individuals or property. This is an atomized way of understanding crime. Instead, I suggest that certain crimes target the human network and are, in ways, worse than other crimes because they harm the community. This is true in realspace as well as in cyberspace, but the language of cyberspace—which focuses on networks and connectivity—allows us to see the point.

Some realspace crimes against networks are obvious. A bomb on a major highway is designed to prevent people from traveling. Even

---

[226] *Id.* at 174.

[227] Eisenberg et al., *supra* note 58, at 258.

though the damage is only to property, it has different effects than a bomb detonated on a private road. Other realspace crimes against networks are more subtle. Think of a shooting at a popular nightclub. Before the shooting, connections between people flourished. People went to the club to have a good time, to meet other people, and to enjoy themselves. But the shooting undermined the trust in the club, and the club eventually was forced to shut down.[228] All of the benefits the club once offered were now lost. Hate crimes, which target a specific group, may also be understood as acts that undermine the community and discourse between its heterogeneous groups. A similar point might be made for rape as well.

What being human means is, in part, interconnectivity.[229] Those crimes that undermine interconnectivity should be singled out for special disfavor, in realspace as well as cyberspace. Cybercrimes such as worms—which clog network connections—are obvious examples of crimes against networks. These crimes are designed precisely to make it more difficult for people to communicate with each other and are analogous to the bombing of a highway in realspace. But there are electronic counterparts to the more subtle forms of crime in public spaces like club shootings. Clifford Stoll's experience with East German hackers breaking into the Berkeley computer systems, for example, demonstrated how a breakdown in trust can poison an electronic community.[230] Because both visibility and tangibility are missing in cyberspace, individuals have even more of a need to trust what they are seeing on their screens. When crimes target that trust, the result can be to prevent people from coming onto the net and to prevent those that do from sharing information. As one researcher put it:

> During the Internet worm attack I experienced problems in my research collaboration with U.S. colleagues when they suddenly stopped answering my messages. The only way to have a truly international

---

[228] This is how a club named Kilimanjaro, near my house, in the Adams-Morgan neighborhood of Washington, D.C., was shut down. *See* Ken Ringle, *The Woes of Kilimanjaro*, WASH. POST, Sept. 25, 1995, at B1 ("'The publicity around th[e] shooting scared everybody away.'").

[229] *See* ARISTOTLE, THE POLITICS, bk. I, ch.2, at 5 (Ernest Barker trans., Oxford Univ. Press 1958) (n.d.) (describing humans as *zoon politikon* or "social animals").

[230] *See* STOLL, *supra* note 48, at 313 ("I learned what our networks are. I had thought of them as a complicated technical device, a tangle of wires and circuits. But they're much more than that—a fragile community of people, bonded together by trust and cooperation. If that trust is broken, the community will vanish forever."); *supra* text accompanying note 48.

> research community is for network communication to be reliable. If it is not, then scientists will tend to stick to cooperating with people in their local community even more than they do now.[231]

A network is, after all, more than the sum of its individual parts. Economic theory predicts that cooperation will yield collective payoffs that are much greater than those derived when individuals only pursue self-interest.[232] A computer network like the internet is nothing more than a structure for this cooperation. Each user derives benefits that exceed those she would otherwise receive, provided that everyone else is similarly cooperating. The trouble with cooperation in practice is that it is very difficult to achieve because the individual gains from defection exceed those derived from cooperation, which is a standard collective action problem.[233] The internet, for example, could not have been built privately because every entity would have waited for another entity to build it first, hoping to free-ride off of the other's hard work. It took the government's sponsorship to build the internet.

Now that this network exists, some forms of computer crime can be understood simply as defections from the cooperative protocols of the net. Computer worms, for example, undermine the positive externalities of the network by making it more difficult for individuals to receive benefits from cooperation. While the payoffs to the criminal may be large (such as when she own a virus-protection software firm or if she has some other interest in preventing communications), the collectivity suffers. The enforcement of computer crime statutes, then, is a way to prevent this harm to the collective network and an attempt to preserve the network's cooperative protocols.

Crimes that target the network, therefore, should be treated differently because they impose a special harm. This harm is not victim-centered, but community-centered, and explains why victims alone should not be able to make decisions about whom to prosecute. We punish not simply because of the harm to the individual victim, but because the crime fragments trust in the community, thereby reducing social cohesion and creating atomization. Just as the law

---

[231] Jakob Nielsen, *Disrupting Communities*, *in* COMPUTERS UNDER ATTACK, *supra* note 55, at 524-25.

[232] *See* ROBERT R. PUTNAM, BOWLING ALONE: THE COLLAPSE AND REVIVAL OF AMERICAN COMMUNITY 288 (2000) ("High levels of trust and citizen participation operate through a variety of mechanisms to produce socially desirable outcomes.").

[233] ROBERT M. AXELROD, THE EVOLUTION OF COOPERATION 7-9 (1984).

must worry about private self-help measures that impede interconnectivity, so too it must worry about private actors who try to sabotage interconnectivity for their own nefarious reasons. Again, while this concept is not one unique to cyberspace, thinking in computer terms, such as network effects, helps us understand it.

4. New De Minimis Crime

Realspace crime control generally depends upon victims to detect and report a crime after it occurs. If John uses a housecleaner to clean his house and that cleaner steals his diamond watch, effective prosecution can occur only once John notices and reports the theft. However, detection and reporting are influenced by the size of the theft—a larger theft is obviously more likely to be reported than a small one (John will detect and report the theft of his diamond watch, but not the theft of pennies left on the floor). Accordingly, the triviality of an offense influences the probability of enforcement. It also may influence whether or not a crime has been committed at all; the de minimis doctrine precludes minor offenses from being considered criminal.

In cyberspace, however, crimes are likely to be skewed and apportioned among many instead of few. Rather than stealing millions from a single bank account, a cyberthief can work by stealing pennies, or even slivers of pennies, from millions of accounts. In so doing, the thief bets that the victims will not notice the missing sliver or have a sufficient incentive to report the matter even if they do notice a discrepancy. Credit card fraud is another example of this type of theft. Instead of stealing one person's credit card number by overhearing it, a cyberthief will steal thousands at once, using each card only a single time so that the crime has a higher chance of going unreported.[234] These types of activities have been dubbed "salami" attacks because the perpetrator is shaving off an imperceptibly small piece of the larger asset.

The existence of salami attacks brings into focus a problem with George Stigler's deterrence analysis. In Stigler's classic article, he argues that the theft of $1000 is more than twice as harmful as the theft of $500.[235] This conclusion might be backwards; because smaller thefts are more difficult to detect, they impose more social disutility

---

[234] John Markoff, *Discovery of Internet Flaws Is Setback for On-Line Trade*, N.Y. TIMES, Oct. 11, 1995, at A1.

[235] Stigler, *supra* note 102, at 529.

than larger ones. One measure of a crime's disutility must be whether its harms are likely to be remedied.

Because victims of crimes in cyberspace are unlikely to notice these types of thefts, and even less likely to report them, law enforcement needs to develop a new model of policing that does not depend as heavily on victims. Instead, the law will need to depend more on institutions that maintain accounts of potential victims, such as banks. These institutions, which monitor multiple accounts, will almost always stand in a better position to detect these forms of theft. For example, they may employ computer hardware and software to trigger alerts whenever a series of accounts is being changed at once.[236] Moreover, accounts could be remotely backed up and checked periodically against current account information to detect discrepancies.

But all of this places law enforcement in uncharted territory. It cannot know what the best, or cheapest, form of protection is for an entity such as a bank. Mandating the use of any particular form of software or hardware is bound to impose deadweight losses given standard failures of bureaucracy, from expertise to capture.[237] Despite these difficulties, it may be possible for lawmakers to create incentives for these entities to detect and report cybercrime. For example, if Jones loses his Visa card and reports it to the company, Jones is only responsible for a small fee, even if a thief uses it to charge thousands of dollars. This strategy places the burden on Visa to create a mechanism that cuts off false charges as quickly as possible. A later Part of this Article proposes similar burden-shifting strategies to create better monitoring among ISPs. Doing so may offset a cybercriminal's ability to conduct simultaneously many thousands of thefts without substantially risking victim detection and reporting.

5. Supersleuth Victims and Electronic Vigilantism

There is, however, a very different role that some victims play in

---

[236] *See* PARKER, *supra* note 18, at 92 ("Victims [of Salami acts] have usually lost so little individually that they are unwilling to expend much effort to solve the case. Specialized detection routines can be built into the suspect program, or snapshot storage listings could be obtained at crucial times in suspect program production runs."); GEN. ACCOUNTING OFFICE, ELECTRONIC BANKING: EXPERIENCES REPORTED BY BANKS IN IMPLEMENTING ON-LINE BANKING 14-15 (1998) (stating that some banks use intrusion detection software to foil attacks).

[237] *See* Lemley & McGowan, *supra* note 220, at 542-44 (criticizing government standard-setting).

some cyberspace crimes. Rather than being passive victims, they become supersleuths, using their computer power to detect, report, and sometimes even punish cybercriminals. For example, when last year's DDOS attacks took place, companies such as eBay aggressively detected them and developed countermeasures. The upshot was that within ninety minutes eBay had developed a filter that permitted the company's web site to function normally again. Other targets of the DDOS attacks joined together to share information about the attacks and to work out solutions.[238]

The emergence of these supersleuth victims heralds new potential for victim-oriented prevention strategies. If there are many victims of a crime in realspace, it is not easy for them to organize. Collective action problems loom, and self-help is quite difficult (particularly when helping augment someone else's security might displace a crime onto your own business or home). In cyberspace, by contrast, it is easier for victims to organize, even as an attack is happening. For example, they can patch firewalls, exchange virus software, and discuss the perpetrator's attack patterns. Indeed, because of the interdependence of the network, it may be optimal for sites to cooperate with each other. If the barriers to victim precaution are lower in cyberspace, then cost deterrence may be more efficient than legal sanctions. This is because victims can prevent cybercrime more cheaply by increasing perpetration costs than the government can through threats of prosecution.

It is therefore possible to envision that cyberspace may alter the relationship between public power and private power, and place more in the hands of the latter. This is not altogether a welcome development. The law enforcement function arises, in part, because society fears private self-help measures. The law, by affording an amount of retribution to the victims of crime, attempts to quell their impulses to take matters into their own hands. But the law is slow, sometimes inefficient, riddled with due process, and often frustrating. Cyberspace is the antithesis of this. Instead of waiting months or even years, ISPs can enact their own forms of crime prevention and justice virtually instantaneously.

We shall call this *the asymmetric incentives* problem, and it is another general quandary in law. The problem arises when the law places burdens on actors that are accommodated by forgoing a benefit with large positive externalities. Here are two examples drawn from

---

[238] *Cyberattack*, Dempsey, *supra* note 182.

realspace. A very robust "hostile environment" test for employment discrimination could lead businesses to terminate any questionable employees, as the benefit from one questionable employee is dwarfed by the liability of a potential lawsuit.[239] A standard of care that imposes drastic liability on employers for torts committed by their employees may lead employers not to hire anyone with even the slightest blemish on their records. A general feature in these two cases is that the burdens placed by the law disregard the way in which law-abiding cautious entities are likely to react.

Reliance on victims to fight cybercrime raises similar issues. If the law places high liability on these parties, the asymmetric incentive problem predicts that they will react by denying entry to questionable users. If Chase Manhattan suspects that someone with a password into the bank system may be a thief, it will deny him access, even on the flimsiest of suspicions. Indeed, the problem is much greater than simply booting an individual user off of a web site. Because that user can simply resurface by opening another e-mail account, some web sites do not just cut off access by a user, they also eliminate access by other users of the same domain system.[240] It will be difficult for the market to prevent these forms of electronic vigilantism when these entities justify their decisions on the basis of protecting other customers. Further, these actions have severe costs. Individuals may be unfairly dismissed, their electronic identities ruined, data may be lost, and interconnectivity may suffer.[241]

---

[239] *See* JEFFREY ROSEN, THE UNWANTED GAZE 79-84 (2000).

[240] If Georgetown University is getting too much spam from AOL, it may try to cut off e-mail sent from AOL, with obvious costs to the users of AOL who want to communicate with the Georgetown community. *See* MAPS RBL Project, *Mail Abuse Prevention System Realtime Blackhole List, at* http://maps.vix.com/rbl (last visited Feb. 18, 2001). The UDP, or Usenet Death Penalty, is another mechanism to accomplish this blocking on Usenet message groups. When UDP is imposed against an ISP, it will block all messages originating from that ISP. *Usenet/Cancel FAQ, at* http://www.landfield.com/faqs/usenet/cancel-faq (last visited Feb. 18, 2001).

[241] The asymmetric incentives problem is one example of a suboptimal self-help strategy. We have already encountered another form of suboptimal self-help, fragmentation on the net and overprotection of web sites. Just as some stores in realspace do not let certain groups of individuals shop in their stores out of a mistaken fear of shoplifting, so too may web sites raise unnecessary restrictions upon entry. These forms of negative self-help suggest that these third parties should not necessarily be given an absolute property right to exclude other users. As Calabresi and Melamed suggest, property rules are appropriate when negotiation costs are lower than the administrative cost of a government adjudication. Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1106-10 (1972). But distributional inequities may arise when one entity is given the power to dictate the terms of a transaction, thus precluding effective

The way in which poor law enforcement on the net is contributing to bad forms of self-help on the part of victims and institutions, or electronic vigilantism, is one piece of the phenomenon we began examining in this Part. Whether the net balkanizes into various enclaves for privileged users, whether a deadweight loss producing an arms race between hackers and victims ensues, and whether institutions will act as private enforcers without due process, or other protections, all depend in part on how the law treats cybercrime. One crucial element, alluded to several times in this Part, concerns the role of third parties.

C. *Third-Party Strategies of Scanning, Coding, and Norm Enforcement*

Unlike crimes in realspace, electronic crimes often involve the assistance of innocent third parties. The author of the ILoveYou worm, for example, used an ISP in the Philippines to spread the disease. Similarly, many computer crimes depend upon credit card companies to provide them the revenue necessary for the crimes to be profitable. This forces us to ask whether lawmakers should develop mechanisms to harness credit card companies as third party intermediaries in preventing cybercrime. One novel way the law could accomplish this is by giving cardholders the right to refuse payment to the card company for illegal transactions. Card companies would then be forced to examine businesses and their products before extending credit arrangements to them.

Even when third parties are not present, they may be in a position to prevent cybercrimes from happening. Here, the chief examples concern programmers and hardware manufacturers. These entities can either pursue destructive ends, such as writing dangerous software like hackers' tools, or they can pursue positive goals, such as building protocols into programs to foil computer attacks. While there are some analogues to these third parties in realspace, their existence in cyberspace is ubiquitous and raises the question of what legal devices optimally situate them in preventing crime. The existence of these third parties is the flipside of the lack of co-conspirators in cybercrime—they are innocent entities that can prevent crime before

---

negotiation. AOL and E*Trade will always be in a position to boot off any potentially risky customers, and this market power means that a liability rule is preferable. Because individual customers may be judgment proof, it may be better to structure the liability rule so that customers could sue to have their membership reinstated, rather than giving customers the right to intrude (and permitting the other entities to sue later).

it happens. Moreover, as repeat institutional players, they may be more responsive to legal risks than are individual users.[242]

1. Internet Service Providers

In cyberspace, there are many reasons to think ISPs may prevent crime at a cheaper cost than the government. In part, this is because the speed of criminal activity in cyberspace suggests legal sanctions will be less effective than cost-deterrence and architectural strategies. The internet gives a criminal the resources to start up a criminal enterprise very quickly, access to millions of potential targets, the technology to reach those targets within moments, and the ability to terminate the enterprise instantaneously.[243] Complicating law enforcement even further is the fact that the criminal may weave his crime through computers in several countries, making investigation even more difficult.[244] While multilateral cooperation among

---

[242] To the extent that government strategies focused on offenders, be they legal sanctions, perpetration cost, or architecture, result in overdeterrence and chill socially beneficial activity, third-party methods are particularly useful. Because many third parties have, comparatively speaking, legal and technical sophistication, they may avoid overreacting to government initiatives.

[243] As Senator Schumer puts it, "[O]ur laws—even our computer laws—are set up for a world that travels at subsonic speed while hacking crimes move at the speed of light." *Internet Denial of Service Attacks and the Federal Response: Joint Hearing Before the Crime Subcomm. of the House Judiciary Comm. and the Criminal Justice Oversight Subcomm. of the S. Judiciary Comm.*, 106th Cong. (2000) (statement of Senator Charles Schumer), http://www.house.gov/judiciary/schu0229.htm; *see also Cybercrime Hearing*, *supra* note 21, at 63 (statement of Jeff B. Richards, Executive Director, Internet Alliance) (claiming that law enforcement must act in "Internet time").

[244] As one FBI official puts it:

> [T]he cyber environment is borderless, affords easy anonymity and methods of concealment to bad actors, and provides new tools to engage in criminal activity.... To deal with this problem, law enforcement must retool its work force, its equipment, and its own information infrastructure. It must also forge new partnerships with private industry, other agencies, and our international counterparts.

Cyberattack, Vatis, *supra* note 25.

The United States has Mutual Legal Assistance Treaties with only a few nations, and the notion of computer crime does not exist in many countries abroad, thereby preventing extradition. *Cybercrime Hearing*, *supra* note 21, at 28 (statement of Louis J. Freeh, Director, Federal Bureau of Investigation). If a country does not punish computer crime, this will often prevent extradition due to the dual criminality doctrine. For example, in 1992 Swiss hackers attacked the San Diego Supercomputer center. The Swiss refused to cooperate with American authorities because of dual criminality, the trail grew cold, and the case was never solved. DOJ REPORT, *supra* note 5, at 41-42.

Cybercrime also brings the notion of extraterritorial regulation to our attention.

governments sounds nice in theory, it is very difficult to achieve in practice. As a result, it may be more efficient for third parties to stop cybercrime from happening rather than to rely on prosecution after a crime takes place.

In a rich article, Reinier Kraakman analyzed the role of third parties in enforcement.[245] He examined three strategies: chaperoning conduct, bouncing offenders, and whistleblowing. Each of these strategies has potential for ISPs. *First*, ISPs can chaperone subscribers by monitoring their conduct. ISPs could randomly monitor web traffic to critically important sites, such as military computers. They may scan web sites hosted on their networks for illegal programs, from pirated software to hackers' tools. ISPs can scan e-mail for viruses, thus stopping their spread.[246] ISPs could also develop sophisticated hacker profiles that permit them to surveil large numbers of users and pick out those who look suspicious because they repeatedly try to enter certain sites.[247] Unlike the old kinds of profiles that invariably and odiously focused on stigmatizing traits such as race or class, the new cyberprofiles will focus on one's acts. This has the potential to revolutionize the fight against crime.

Second, ISPs could bounce risky subscribers by purging them from the network altogether. They could, for example, bar customers from opening accounts without realspace identification, such as drivers'

Larry Lessig explains the prohibition of crimes committed abroad on the ground that someone who engages in criminal activity in other countries is more likely to engage in it upon return to America. LESSIG, *supra* note 4, at 191. This explanation, however, omits a more fundamental reason for criminal law to cover extraterritorial acts. The law prevents certain crimes abroad not only because of the complementary relationship with crimes that might eventually take place domestically (which is Lessig's point), but also because such crimes reflect poorly on the world's opinion of the United States and its population. From this perspective, the government regulates crimes in order to preserve and protect the reputations of U.S. citizens.

[245] Reinier H. Kraakman, *Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy*, 2 J.L. ECON. & ORG. 53 (1986).

[246] *See* Barbara Cole-Gomolski, *E-Mail Getting a Scan from Server*, COMPUTERWORLD, Nov. 24, 1997, at 53 (discussing server-based scanning programs that detect viruses before they reach the end-user's desktop); Christopher Lindquist, *You've Got (Dirty) Mail*, COMPUTERWORLD, Mar. 13, 2000, at 72; Juan Carlos Perez, *ENS Offers E-Mail Virus Scanning*, *at* http://www.computerworld.com/cwi/story/0,1199,NAV47_STO24841,00.htm (July 15, 1996) (discussing an ISP's e-mail scanning service that detects and quarantines infected files); Sarah L. Roberts, *First Line of Defense*, *at* http://www.zdnet.com/pcmag/features/utility/emailav/_open.htm (Apr. 8, 1997) (reviewing and testing various e-mail anti-virus gateway applications).

[247] According to Dr. Fred Cohen, the person who, in 1983, coined the term "computer virus," internet crime can be stopped by creating generic threat profiles. *Cyberthreats*, Cohen, *supra* note 121.

licenses, thus crippling digital anonymity. *Third,* ISPs could act as whistleblowers and report instances of computer crime. The trouble with whistleblowing, as Kraakman points out, is that it often imposes large costs because it forces targets to hire legal counsel and expend resources.[248] In cyberspace, however, the reporting requirement might be most effective when ISPs report their findings not to the police, but to private entities. For example, ISPs could create tiers of trustworthiness and place each subscriber in a specific tier based on activity patterns. That tier would be furnished to those web sites and users interacting with a particular subscriber, and the sites and other users can thus decide whether to engage in transactions given the risk designation. But there are obvious costs to this strategy, including harms from false negatives and positives.

Fourth, and moving beyond Kraakman's three categories to usher architecture into the analysis, ISPs could build software and hardware constraints into their systems. They may, for example, ensure that electronic traffic carries a specific source address consistent with the assigned address (a technique called egress filtering). ISPs might go further and only accept traffic from authorized sources (a technique called ingress filtering).[249] Or ISPs could configure their systems to prevent subscribers from repeatedly trying to log in using different passwords.[250]

Fifth, ISPs could use methods that make it easier for law enforcement to investigate cybercrime. These techniques would not only help solve crime ex post, they would also help deter crime ex ante. For example, ISPs could preserve data trails for long periods of time, thus enabling the government to trace electronic signals.[251] Or they could agree to pierce digital anonymity upon a sufficient showing

---

[248] Kraakman, *supra* note 245, at 59. ISPs must currently notify authorities if incidents of child exploitation come to their attention. *See* 42 U.S.C.S. § 13032 (Lexis 2000).

[249] *Cyberattack,* Fithen, *supra* note 211. While ISPs have claimed that ingress filtering "would make their systems unmanageable or too slow, such networks as the @Home Network now operated by AT&T, which is [at a] far higher speed than the vast majority of ISP connections today, have adopted this practice with great success and without apparent management or cost effects." *Cyberthreats,* Cohen, *supra* note 121.

[250] These strategies raise transparency concerns, and will be discussed *infra* text accompanying notes 265-71

[251] Data-preservation letters pursuant to 18 U.S.C. § 2703(f) permit the government to request that an ISP "take all necessary steps to preserve records and other evidence in its possession pending issuance of a court order or other process." 18 U.S.C. § 2703(f)(1) (Supp. IV 1998). Such records are to be preserved for ninety days, and the period can be renewed for another ninety days. *Id.* § 2703(f)(2).

by the government of the need to do so.[252]

Should law require ISPs to use these five strategies? Not always, because following the strategies may incur deadweight losses that outweigh their utility. Just as with victim precaution, ISPs are not always the cheapest cost avoiders. Virus scanning software, for example, is costly, may slow systems down considerably, and can threaten individual privacy interests. ISPs that require subscriber information might pose a threat to privacy, either because they might leak the material themselves or because a rogue employee or hacker might do so. If ISPs were liable for pirated material on their networks, they might more vigilantly police subscribers to the point where privacy would be eroded.[253] And the perception, often unwarranted, that the government has broad surveillance powers may exacerbate the public's fears of loss of privacy. This is one example of the asymmetric incentive problem as applied to ISPs. If ISPs are liable for the sins of their users, they will purge anyone about whom they have the slightest suspicion of committing criminal wrongdoing. When AOL suspects that Smith spread a virus, even unintentionally, it will eliminate Smith because the benefit to AOL of one additional customer will be outweighed by the risk of harboring a virus-spreader.

The point of these quick examples is not to suggest that third-party deterrence is always inappropriate, but simply to caution that there are tough calculations to work out. Because government is usually unlikely to have information about optimal third-party precaution, it should not use sanctions to force ISPs to engage in particular forms of prevention. (Some European countries, by contrast, consider it a crime to operate a computer center without adequate security precautions.[254]) The government is likely to over- or

---

[252] The government could, for example, use contract law as a way of enhancing compliance with criminal law. It could require that contracts between an ISP and a subscriber contain a provision permitting the ISP to expose the real identity of a user after a sufficient government request. Such contractual relationships would not emerge in a free market due to free rider problems. A Dutch proposal, by contrast, would punish an ISP that could not identify the actual offender in certain cybercrime cases. Ulrich Sieber, *Responsibility of Internet Provider—A Comparative Legal Study with Recommendations for Future Legal Policy*, 15 COMP. L. & SEC. REP. 291, 302 (1999).

[253] An Australian High Court decision suggests that ISPs will be liable for copyright infringement on its networks. Telstra Corp. v. Australasian Performing Right Ass'n, 71 A.L.J.R. 1312, 1319 (Austl. 1997); *see also* Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 WL 323710, at *5 (N.Y. Sup. Ct. May 24, 1995) (holding Prodigy liable for defamation because its editorial control over statements "opened it up to a greater liability than . . . other computer networks that make no such choice").

[254] Sieber, *supra* note 252, at 293-96.

underestimate the costs and benefits of prevention, and this runs the risk of either prompting actors to forgo utility-producing activity or inducing them to take wasteful precautions.

Government thus should recognize that it lacks information about proper third-party crime prevention. Yet ISPs may at times be the cheapest cost avoiders, and forgoing their assistance risks inefficiencies and a loss in deterrence.[255] (For example, the State of New York recently brought an indictment against an ISP that failed to prevent its members from accessing child pornography; bringing this single action might do more to reduce child pornography than bringing numerous actions against the ISP's customers.[256]) The difficulty lies in writing legal rules that recognize this efficiency. The common solution to the lack of government information is to use the tort system and a standard of "due care."[257] Forcing every ISP to determine the costs and benefits of due care, however, imposes the deadweight loss of each ISP having to run such calculations. Instead, government may subsidize the development of a common set of standards partially devised by industry. The failure to adhere to these standards could give rise to civil liability.[258] An ISP could be responsible for a small portion of damages caused by a subscriber if the damage could have been prevented with due care; such due care would be defined by industry standards.

This is one method to create downstream liability for ISPs that do not take reasonable care. The case for doing so is that ISPs do not

---

[255] *See* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 437 (stating that in "situations in which the imposition of vicarious liability is manifestly just, the 'contributory' infringer [is] in a position to control the use of copyrighted works by others and [has] authorized the use without permission from the copyright owner" (citations omitted)).

[256] *See BuffNET Enters Guilty Plea in Porn Case*, BUFFALO NEWS, Feb. 17, 2001, at A7.

[257] Due care, however, can be difficult to define. It should include all the factors in the Hand formula, *see supra* text accompanying note 223, as well as the social costs of third-party precaution.

[258] Larry Lessig has suggested that ISPs could create disincentives for people viewing inappropriate sites, such as "slowing the response time for a certain kind of service it wants to discourage." LESSIG, *supra* note 4, at 71. Lessig's idea here is largely critical, but it can be used to explore the ways in which ISPs might be used to fight cybercrime. Because no one ISP has an incentive to reduce criminal activity, a serious free rider problem exists; any ISP that tries to reduce crime through slowing down response times or verifying identities would simply leave a would-be criminal to switch service providers. If the government, however, required ISPs to monitor subscribers, the free rider problem would be minimized. ISPs may be in the best position to monitor criminal behavior since they are most familiar with traffic patterns, identities, and other important information.

have market incentives to behave as gatekeepers and that for them to behave in this way generates positive externalities.[259] These externalities, which increase perpetration costs and architectural barriers to crime, are important because legal sanctions provide only a portion of deterrence. Government regulation of ISPs is necessary to avoid free riding (for example, CompuServe might not install virus-filtering software because it hopes that AOL will) and to bring about efficient third-party prevention. This is why relying on custom will not yield an efficient result; custom may arise because of a race to the bottom rather than because it is optimal.

Nonetheless, any use of the tort system must account for the asymmetric incentive problem. Placing burdens on ISPs risks balkanizing the net and inducing ISPs to purge risky users. Again, these results might be worth the cost; the point is simply that this can become part of the price tag. It is therefore necessary that assessments of ISP liability incorporate the full social cost of prevention before they are employed. A formula that simply compares an ISP's cost of prevention against the harm of the crime would ignore these other important costs. Lowering the amount of damages, say to a fraction of the ultimate harm, may be one way to maintain security incentives without incurring suboptimal preventative costs.

But the costs of third-party prevention mechanisms must not blind us to the fact that ISPs will often be essential in preventing cybercrime. The failure to rely on ISPs to prevent cybercrime threatens enforcement of the law. Because cybercriminals can coordinate simultaneous attacks and overwhelm traditional law enforcement, ISP participation is often necessary. This dilemma is an example of Larry Lessig's claim that "a difference in degree [can] ripen into [a] difference in kind."[260] While Lessig does not fully explicate his claim, cybercrime illustrates it well. Computer attacks come not in single instances, but in great numbers, and all at once. To prevent crime on the net, law enforcement will need to harness private self-help measures, such as firewalls, to create a responsive, quasi-living network that permits private actors to band together and stop attacks through architectural and cost-based solutions. Law faces

---

[259] Hackers do not hack only into an ISP's computers, and viruses do not simply spread among an ISP's subscriber base. Therefore, the benefits of ISP prevention do not inhere only to the ISP, whereas the costs (such as higher access fees, slower response times, etc.) are foisted on subscribers.

[260] LESSIG, *supra* note 4, at 21.

a difficult task in trying to encourage enough third-party precaution to prevent cybercrime, but not so much that the benefits of the net are undermined.

2. Credit Card Companies

Many cybercriminals use a profit model that depends on credit card companies. To remain viable, sites that distribute pirated software, illegal child pornography, or hackers' tools need profit. (I intentionally place not-for-profit cybercrimes, such as the free release of copyrighted music, to one side.) For a large number of these crimes, credit card companies are the predominant method of payment. This is because of the enormous transaction costs involved with alternatives, such as sending cash through the mail (slow and traceable) and digital cash (not really available yet, and perhaps always traceable, depending on the code). For this reason, credit card companies, which are currently third-party beneficiaries to these forms of computer crime, may be a useful ally in preventing them.

The trick is to create a system that will encourage credit card companies to refuse credit services to illegal businesses. Card companies plead ignorance when faced with situations in which their customers are found to be engaging in felonies. This ignorance, or perhaps willful blindness, is widespread, and because the majority of card companies do not have actual knowledge of their customers' business practices, it is difficult to charge them with a criminal violation. Instead, a simple change to the rules of payment may provide card companies with an incentive to avoid blindness and reduce criminals' ability to rely on card-generated profits.

The simple trick is to give credit cardholders the right to refuse to pay for items on their bill that are illegal. Credit card companies already investigate disputed items, such as when a vendor overcharges a customer. The rule change would add illegality to the list of items that require investigation. Because card companies would fear extending credit to companies for services that might go unpaid, they would have an incentive to investigate the business practices of each client. The deadweight losses incurred by investigations would have to be assessed against the cost of computer crimes; if the losses are too great, then perhaps the rule could be modified so that only certain forms of illegality would give cardholders a right to refuse payment, thereby reducing the frequency, extent, and cost of card company investigations. Good faith investigations and monitoring by card companies could also serve to nullify a customer's refusal to pay. The

method would reduce the gain to offenders by steering crime into less efficient modes, requiring greater investments to receive profit from customers. This is one example of using civil regulation on noncriminals to alter a variable that deters crime: perpetration costs.

3. Software and Hardware Manufacturers

In addition to interfering with payment, the government can induce software and hardware manufacturers to employ architectural strategies that further deter cybercrime. For example, the government could require that hardware routers be modified to detect and eliminate suspicious traffic.[261] Government could also require software manufacturers to remove trap doors or to provide accurate information about their existence. Or the government might regulate the net more directly by encouraging or requiring the installation of more secure code, such as Internet Protocol Version Six.[262]

In general, regulating software programmers will reduce enforcement costs (as compared to regulating end users) because there are fewer programmers than end users. A single enforcement action against Napster, for example, might deter more copyright theft than prosecuting hundreds of individual users (particularly when programmers as sophisticated repeat players may be more responsive to legal risks than are individuals). The technique of product regulation as crime control is sometimes available in realspace, such as when the government regulates the sale of harmful products like firearms and thieves' tools because they may be used to commit crimes. At times, government's realspace strategies are subtle—such

---

[261] *See Internet Denial of Service Attacks and the Federal Response: Joint Hearing Before the Crime Subcomm. of the House Judiciary Comm. and the Criminal Justice Oversight Subcomm. of the S. Judiciary Comm.*, 106th Cong. (2000) (testimony of Charles Giancarlo, Senior Vice President, Cisco Systems, Inc.), 2000 WL 234739 [hereinafter *Cyberattack*, Giancarlo] (stating that internet switches and routers "can be equipped with a variety of filters and security devices that detect suspicious patterns in the information traffic at a site," and that such "equipment can be configured to limit or entirely block out data that appears suspicious" and "can be . . . configured to sniff out these phony addresses and break off contact before a traffic jam results").

[262] This protocol, which is nearly complete, would revamp the old web protocol codes by requiring each data packet to "carry its own authentication and encryption." Holman W. Jenkins, Jr., *Some Things Are Worse Than a Woolly Web*, WALL ST. J., Feb. 16, 2000, at A27. Thus, it would foil DDOS attacks as well as carry the possibility of enhancing law enforcement's ability to trace criminals who use the internet in furtherance of their crimes.

as changing highway patterns to foil certain crimes.[263] These are all methods that employ cost deterrence principles by making it expensive for a criminal to pursue illegal activity.

Direct government regulation of hardware and software will not generally create an asymmetric incentive problem in the way reliance on ISPs and victims does. This is, in part, because government strategies will not rely on unknown quantities of civil liability. Obviously, if an e-mail company could be held financially responsible for the spread of a virus, or an internet browser company could be found liable for a virus spread through its product, the result could be to close down these businesses and stymie future innovation. For that reason, government may forgo civil liability and regulate certain basic forms of security measures by making the failure to follow them subject to low, not open-ended, administrative fines.

The problem with such a strategy is that the government often lacks data about necessary security protocols and is even more unfamiliar with their costs.[264] The government has a natural tendency to favor security over operability (a different type of asymmetric incentive problem). For that reason, government must make its code regulations available to industry ahead of time, so that industry has an adequate chance for notice and comment. The trouble with following this procedure is that notice might tip off criminals, who can use the time to develop countermeasures to bypass the proposed security protocols. Security and operability thus may be, in reality, mutually exclusive goals.

This tension between security and operability is a difficult one to accommodate and a third factor must be considered as well: transparency. Hardware and software protocols are embedded, often invisibly, in computers. Larry Lessig has argued that it is difficult for the public to hold government accountable for regulations it imposes on manufacturers. Law enforcement has the obvious goal of avoiding giving criminals open access to its designs, but pursuing this goal,

---

[263] *See supra* text accompanying notes 13, 98-107 (discussing realspace strategies for crime control, such as increasing perpetration costs or modifying architecture).

[264] *See supra* text accompanying notes 200-01 (indicating that investigating and prosecuting each and every of the millions of cybercrimes committed is not an economically viable option). There are times, however, when the government might be ahead of the private sector in developing software to forestall attacks. For example, the FBI developed a software measure that could detect DDOS agents and masters on operating systems. It made the detection tool available on its web site, and it has been downloaded "tens of thousands of times," preventing many such attacks. *Cyberattack*, Vatis, *supra* note 25.

Lessig contends, can strip necessary information from the law-abiding public as well. Citizens cannot vote with their purchases if their purchases contain secret code. And even if they know of the code's existence, they will not know whether the manufacturer or the head of the FBI insisted on it. Thus far, we live in a system in which abuses by prosecutors and police are generally checked by the electorate; if you do not like what district attorney Robert Morgenthau is doing you can vote him out.[265] But the regulation of code in cyberspace, Lessig claims, threatens this structure of accountability and also creates the potential for public paranoia about law enforcement on the net.

There are some flaws with this explanation. After all, law enforcement in realspace does not have transparency either. Think of informants, undercover cops, and many secret law enforcement techniques such as interrogation methods. (Indeed, many regulations that govern realspace in the administrative state are made by largely unaccountable agencies as well, in matters of crime control as well as numerous other areas.) It is at least debatable as to whether government regulation of software and hardware would be less transparent than these realspace regulations.[266]

Perhaps the largest flaw with the transparency argument against government regulation is that it confuses the causality; government regulation may actually solve the transparency problem rather than cause it. Code, after all, is largely written by private entities. The choices made by programmers have policy implications, e-mail programs can be configured to turn sensitive information over to

---

[265] LESSIG, *supra* note 4, at 98 ("The state has no right to hide its agenda. In a constitutional democracy its regulations should be public. And thus, one issue raised by the practice of indirect regulation is the general issue of publicity. Should the state be permitted to use non-transparent means when transparent means are available?"); *see also id.* at 7, 18, 44; Lawrence Lessig, *The Law of the Horse: What CyberLaw Might Teach*, 113 HARV. L. REV. 501, 541-43 (1999) (contending that secret regulation of code would diminish political accountability and enable the government to "avoid the political consequences of its choices").

A different argument against over-reliance on code-based regulation emphasizes trust. An emerging body of empirical evidence suggests that cooperation can be enhanced by institutions that foster and support trust rather than rely solely on overt regulation. *See* Margaret M. Blair & Lynn A. Stout, *Trust, Trustworthiness, and the Behavioral Foundations of Corporate Law*, 149 U. PA. L. REV. (forthcoming 2001). If the architecture of the internet shifts to one in which users are presumed to be nontrustworthy, its presumptions could prove self-fulfilling.

[266] One difference is that these structures of constraint generally only target lawbreakers, whereas certain forms of code regulate everyone. But this difference may cut the other way; greater accountability may inhere to those regulations that govern lawabiders and lawbreakers alike.

government agents and private detectives, web pages can secretly collect information about users and distribute it to commercial entities, and so on. Transparency is not a concern acute to government regulation; private code too has such drawbacks. Viewed from this perspective, government regulation of source code might actually further transparency goals. Government regulations are required to be public, placed in the United States Code and the Federal Register. And the Freedom of Information Act ("FOIA") is a broad weapon to counter any indirect government mechanisms to regulate cyberspace. Through public rules and FOIA, government regulation can shed sunlight on private code. (Other mechanisms, such as open hearings, notice and comment proceedings, open votes in Congress, and public trials shed further light as well.)

For government regulation to further transparency goals, the regulations themselves—but not necessarily the precise source code—must be made public. There are ways to structure a system that would further enhance accountability, such as by insisting that any government regulation be placed in the United States Code, rather than in an agency regulation, and devising a substitution procedure that permits the public to be on notice of a regulation's effect, without providing the technical details of the code.[267] Alternatively, a panel of private experts could be given the underlying source code if the details were truly necessary to evaluate the system. Open regulations could also make it easier for industry to participate in their formulation and thereby assist the government in devising an optimal policy.[268]

The transparency problems with direct government regulation

---

[267] The substitution proposal could be modeled on § 6(c) of the Classified Information Procedures Act, 18 U.S.C.S. App. § 6(c) (Lexis 2000).

[268] Legal scholars generally think of administrative and criminal law as separate spheres, but there are a host of regulations that intersect these two areas. Sometimes the safety component of these regulations is not always apparent from the plain text (for example, a rule requiring lighting around taverns). Instead of regulating software and hardware manufacturers, for instance, government could devise security standards that insurance companies should use when devising liability policies. These companies would be free to depart from such standards if they deemed them over- or underinclusive, and this practice might lead to a more efficient result than simple regulation. "Cyberinsurance is the hottest sector in the insurance industry" right now. Banham, *supra* note 1; *see also Cyberattack*, Giancarlo, *supra* note 261 ("In the 'bricks and mortar' world, retail businesses take advantage of lower insurance rates if their stores are adequately protected with locks and alarm systems."). These companies have a profit incentive and may be best situated to adapt to changing technology. Alternatively, government may provide tax breaks for internet companies that undertake certain security measures.

have been overstated and the severe change the computer has wrought in the ease of crime may force consideration of such solutions. Regulating a few software manufacturers will often prove easier than regulating one hundred million users. If browsers could not pirate music, for example, the cost of engaging in piracy would be much higher to individuals (yet another example of cost deterrence).[269] Even if individuals did not know that code was constraining their activity, they would inevitably be affected by the software protocols that the code writers developed and their tastes may be shaped away from illegal conduct by the unavailability of pirating software.[270] Of course, government must be sensitive to its institutional weaknesses and avoid using fiat in ways that create inefficiencies. Nevertheless, regulating code provides the government a new, and important, mechanism for deterring criminal activity.[271]

4. Public Enforcement of Social Norms

Thus far, we have seen how third parties can control crime through increasing the probability of detection by law enforcement,

---

[269] This is what the law has currently attempted to do by forbidding rewritable CD players that can make copies of copies. 17 U.S.C. § 1002(a) (1994).

[270] *See supra* notes 195-98 and accompanying text (discussing adaptive preferences and how they affect the development of crime on the internet). However, the use of code must be attentive to constitutional constraints, constraints that are beyond the scope of this Article.

[271] If a secure code is necessary to prevent crime, it may follow that some forms of computer crime may generate utility. Computer crimes such as launching viruses and hacking can test the limits of security; these actions may at times contribute to the general welfare. For this reason, the estimates that the ILoveYou worm caused more than $10 billion in damages are overstated. The episode revealed the security weaknesses in the popular Microsoft Outlook program and underscored the fact that the cookie-cutter software programs that run on most of the world's PCs are fraught with homogeneity. If there were greater variety in e-mail programs, for instance, the virus could not have spread nearly as rapidly as it did. But because virtually everyone (for now, at least) uses Outlook, the virus spread from Manila to Milan in minutes. As any farmer knows, genetic variety is vital in protecting against the spread of crop disease. The Irish potato blight of the 1840s was caused, after all, by a monoculture which permitted the disease to spread like wildfire. Harold J. Morowitz, *Balancing Species Preservation and Economic Considerations*, 253 SCIENCE 752, 753 (1991). Just as variety in DNA codes is important, so too is variety in computer software codes. Like an infection in realspace, the upshot of the ILoveYou worm may be to bring about a stronger immunity for our computers in times to come. This is not to say that such behavior is forgivable or even a good idea, only that there are complicated effects stemming from these forms of computer crime. Optimal third-party strategies must bear in mind that, just as the social costs of prevention tend to be underestimated, so too the costs of computer crime tend to be exaggerated.

increasing perpetration costs, and modifying architecture. We now take up the matter of whether it is possible to use the general populace—a diffuse third party—to enforce social norms against crime.

In realspace, norm-based strategies are promising because crime is almost always visible. The perpetrator must come to the scene of the crime (say, in a car), the victim and other witnesses may see the perpetrator (a man holding a large wrench near a windshield), the commission of the crime itself is visible (the man putting the wrench through the windshield), and the after-effects of the crime are visible (the smashed glass, the stolen car). The architecture of cyberspace, however, alters these parameters. The criminal may be thousands of miles away, no witnesses may observe the criminal's presence, the crime itself may be masked by layers of code, and the after-effects of the crime may take months or years to even discover. All of this poses challenges to the realspace model of law enforcement.

a. *The Influence of Social Norms*

In realspace, crime is controlled not merely through the threat of police sanction, but also through the development of social norms that constrain lawbreaking. The police cannot be present to prevent every crime (nor would we want them to be). Instead, effective law enforcement requires the internalization of the lessons of the law by a large majority of the population, even in circumstances in which the police are not near. Social norms have two aspects: they prevent people from engaging in criminal activity through the development of conscience *and* they embody a system of values that society enforces. These values transform individual citizens into projectors of conscientiousness for others. In short, the law helps social norms develop, and these social norms constrain criminal activity.

Larry Lessig has suggested that the lack of physical presence and concrete identity hamper the efficacy of regulation through social norms in cyberspace.[272] Because people can change their identities at will and are not necessarily who they say they are, it is quite difficult to hold them accountable for their past actions on the net.

---

[272] LESSIG, *supra* note 4, at 15-17. The lack of norms in cyberspace may also be an outgrowth of the newness of cyberspace. The codes of conduct that govern realspace have evolved over decades, if not centuries. In contrast, there is no consensus regarding what counts as good conduct on the internet. *See* Rasch, *supra* note 18, at 145.

Furthermore, the ethic of cyberspace, which encourages roleplaying and alternative characters, facilitates the erasure of norms. When only a few people owned computers, and when even fewer of these owners were hackers, codes of conduct evolved to constrain much cybercrime. However, just as regulation by social norms becomes ineffectual in vast, anonymous metropolises, so too the vast expansion of the net has eroded these codes.[273]

On the other hand, while much has been made about the lack of norms in cyberspace, it is worth asking why more cybercrime does not take place. It is not difficult to break into a computer, but the majority of people refrain from doing this. One reason for such restraint is because they think such behavior is immoral.[274] If so, an understanding of how morality and conscience act as constraints in the invisible world of cyberspace must be developed. This understanding would start with the fact that no crime can be committed purely in cyberspace; every crime requires some user who lives and breathes in the physical world. And it is here that the role of social norms emerges.

Because crimes committed in cyberspace still require a user to be in realspace, law can bring realspace institutions to bear in preventing cybercrime. By helping citizens act as norm enforcers, law can contribute to private prevention efforts while simultaneously working to entrench certain norms into the conscience of individuals. Computer criminals may be observable while committing a crime, and

---

[273] There is strong evidence that this is the case, from the rise of hate mail on the internet to the number of online affairs and other behavior typically constrained by norms in realspace. *See, e.g.*, Chris Brooke, *I'm Losing My Man to an American He Met on the Internet*, DAILY MAIL, June 21, 2000, at 29; Libby Copeland, *Cyber-Snooping into a Cheating Heart*, WASH. POST, Aug. 8, 2000, at C1 (describing the unraveling of a marriage due to an online romance); John Markoff, *Staking a Claim on the Virtual Frontier*, N.Y. TIMES, Jan. 2, 1994, at E5 ("I'm in mourning. . . . We once had our own code of honor. Now there's a land grab going on in cyberspace. I'll just have to put up bigger walls and get better alarms.").

[274] [T]he behavior of people in cyberspace is strongly bound by social norms, albeit perhaps not so much as in [realspace]. . . . Technically knowledgeable friends of mine have assured me . . . that even those systems rated as secure against crackers are far more vulnerable than they ought to be. Cracking tools are widely available. The recent Denial of Service attacks on Yahoo and others now appear to have been carried out by someone whose technical competence was meager. And so it would appear that the same sort of social pressure that makes it reasonably safe to walk around in a city full of bricks, makes it reasonably safe to have computers on an Internet infested with crackers.

E-mail from Neal Stephenson, Author, to Neal Katyal, Associate Professor of Law, Georgetown University Law Center (Apr. 28, 2000, 01:07 EST) (on file with author).

they are certainly observable afterward. Strategies that teach children about the evils of cybercrime might therefore function well, not only because children may internalize the lessons and believe that cybercrime is wrong, but also because they may listen enough to feel guilty after committing one. This guilt is likely to emerge when seeing parents and peers.

Lawmakers can capitalize on the deterrent effect of social norms in several ways. Low technology techniques such as placing computers in visible locations can also reinforce the visibility of the user and computer screen and thus cut down on cybercrime. (Perhaps the law could require internet cafés and other vendors to place kiosks in visible areas.) In addition, technologies might be developed to transmit authentic facial displays between users as a way of mirroring transactions in realspace. Again, the idea is to harness the realspace elements that exist in any cybercrime and to bring the social norms that constrain crime to bear on those elements.

Law enforcement cannot simply see its task as prosecuting crime as it happens. Rather, it must proactively educate citizens about the dangers of cybercrime and try to facilitate the use of social norms as a constraint. Because the architecture of the net enables relative invisibility and pseudonymity, such a task is not easy. But using the realspace monitoring and inculcation provided by parents, peers, and others may prevent some crime on the net. While such strategies will not be completely effective, they may aid in deterring a segment of the offending population—a segment that may not be as responsive to legal sanctions or monetary prices.

b. *Broken Windows in Cyberspace*

Forgive the linguistic play, for "broken windows" refers not only to the theory of policing developed by James Q. Wilson and George L. Kelling,[275] but also to what happens to a computer after being exposed to a strong computer virus that disables the Microsoft operating system. Apart from this verbal coincidence, what does Wilson and Kelling's theory tell us about criminal law in cyberspace? At first glance, one is tempted to answer "nothing at all." After all, unlike crimes in realspace, those in cyberspace are almost always invisible. There are no bars on the windows to glimpse and no loiterers and panhandlers to avoid. Broken windows is a metaphor for realspace

[275] *See* James Q. Wilson & George L. Kelling, *Broken Windows*, ATL. MONTHLY, Mar. 1982, at 29.

policing, not one for the invisible world of computer-created space.

But this impulse is wrong. The idea behind the broken windows theory is one about the complementarity of crime, that visible disorders should be punished because they breed further disorder.[276] The insight of Wilson and Kelling was that these disorders are not always the most serious crimes like murder and rape, but instead could be as trivial as loitering and littering. Wilson and Kelling thus inverted the standard thinking about enforcement and suggested that it was more profitable to focus on low-level crime. The reason for this shift in focus, however, was the idea of complementarity between crimes. As crimes become more common, the norms that constrain crime erode, and more crimes take place as a result of that erosion.

A theory that adapts broken windows to cyberspace, therefore, would begin by asking what types of computer crime produce complementarity. It turns out that most of the widely reported and publicly known computer crimes, such as Robert Morris's worm and the recent ILoveYou bug, prompted rashes of copycat crimes.[277] To avoid copycat crimes, law enforcement must punish, rapidly and powerfully, those crimes that produce the most visible social disorder in cyberspace. While this sounds intuitive, it has some perverse results. It may mean, for instance, that government should not expose some criminal activity to public view and ought to maintain the invisibility of such crimes.

Many corporate victims do not report cybercrime to the police because they fear alerting customers and shareholders to the lack of security.[278] Because only the corporation has the data revealing the

---

[276] *See id.* at 31 ("[O]ne unrepaired broken window is a signal that no one cares, and so breaking more windows costs nothing.").

[277] *See Internet Integrity and Critical Infrastructure Act: Hearing Before S. Comm. on the Judiciary*, 106th Cong. (2000), LEXIS, Federal Document Clearing House (statement of James K. Robinson, Assistant Attorney General for the Criminal Division) ("Frighteningly, the 'I Love You' virus was followed almost immediately by copycat variants. [Among the] almost 30 . . . variants that . . . followed . . . [was] the New Love virus, a virus that self-replicated, mutated in name and size, and destroyed the computer systems affected by it."); Pamela Samuelson, *Computer Viruses and Worms: Wrong, Crime, or Both?*, *in* COMPUTERS UNDER ATTACK, *supra* note 55, at 479, 484 (mentioning reports of copycat activity following publicity of Morris's worm).

[278] William J. Cook, who authored the DOJ's computer prosecution manual, states that "[o]rganizations often swallow losses quietly rather than notifying the authorities and advertising their vulnerability to shareholders and clients." Michael Lee et al., Comment, *Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal*, 14 BERKELEY TECH. L.J. 839, 844-45 (1999) (citation omitted); *see also Cyberthreats*, Cerf, *supra* note 23 ("Companies are concerned that revealing and admitting past mistakes, shortcomings, negative experiences or incidents can open

crime, no one else is likely to discover it. Government might want to keep some forms of crime invisible—not only in order to encourage victims to come forward, but also to prevent social disorder wrought by complementary crimes.[279] Since these crimes may only affect individual entities (putting to one side situations in which viruses replicate and spread to other computers), prosecution of these cases should be a low priority because they do not create harmful complementarity. Building on the experience of victims, the government could occasionally release reports about how to maintain effective computer security. Therefore, government may want to create mechanisms to permit victims of crime to inform the government so that investigators can conduct adequate studies about them, but also guarantee the secrecy of the victims.

Traditional broken windows theory suffers another dissimilarity with cyberspace: geography. Underlying Wilson and Kelling's theory is a second idea stemming from Wilson's earlier work, that law-abiding residents move out of high crime areas and thus leave them for criminals to plunder.[280] One goal of criminal law should be to encourage good neighbors to live on every street corner. Broken windows policing accomplished this by cutting down on visible problems, thus making law abiders feel secure. In cyberspace, however, there are no geographic areas or boundaries. Instead, law must encourage the equivalent of good neighbors to flourish by punishing even those minor computer pranks that achieve high visibility. The Morris worm, for example, did not destroy any data. Nevertheless, it scared off a whole group of people from using computers, and may have even stymied the growth of the net. The more law-abiding people that exist on and off the net, the greater the power of norm-based regulation.

---

them up for [public] criticism [or potential legal liability]. . . . [C]ompanies are [also] loath to share proprietary or privileged corporate information. Additionally, firms run the risk of eroding consumer, customer, partner and investor confidence.").

[279] There may be instances in which the government needs to disseminate information quickly about a particular crime to permit other users to take countermeasures against a specific form of attack. While publication of these methods often carries the cost of teaching other criminals how to carry out the crime, law enforcement generally issues the warnings. *See* PARKER, *supra* note 18, at 39 ("The FBI, Scotland Yard, and many other police agencies publish criminal records. The justification is that a net benefit results from forewarning potential victims so that they may defend themselves, even though the enemy may be aided as well."). Such warnings are generally appropriate if they do not jeopardize the flow of information between law enforcement and individual victims.

[280] *See* JAMES Q. WILSON, THINKING ABOUT CRIME 20-37 (1975).

CONCLUSION

For several years, the dreams of technological promise and the specter of technology-driven disaster have threatened to collide. The net is becoming an engine of personal, professional, and economic growth, but, because of this growth, new dangers loom. The first months of the new millennium aptly demonstrated these dangers; two crimes that imposed some of the largest economic losses from crime in history were launched from a few private computers. Ironically, these attacks took advantage of what all of us like about computers: their speed, efficiency, trustworthiness, and low startup costs. As criminals become more sophisticated about such attacks, the incidence of these crimes will rise and criminals' escapes will multiply. Law must counter this trend by embracing new strategies that harness the legal and nonlegal constraints on crime.

This Article has suggested four such strategies, although many more are possible. *First,* law must recognize that an unintended byproduct of computers is that they serve as substitutes for conspirators. Because conspirators sometimes provide benefits to law enforcement, by becoming informants or cooperating witnesses, the government must devise strategies that recognize the fact that these benefits are lost when this substitution occurs. One such strategy, as I have explained, is to treat computers as quasi-conspirators.

Second, law should recognize that certain technologies, such as encryption and anonymity, have dual purposes. Rather than postulating that they are entirely deleterious and punishing them wholesale, society must understand that these technologies can be used for both good and bad ends. To accomplish this balance, the law should develop sophisticated sentencing enhancements and other nuanced strategies such as specific exclusions, and forgo the blunt sword of total prohibition.

Third, the government must increase the financial cost of crime, and the skills necessary to commit it, by placing some responsibility on third parties, such as ISPs, and even on victims. But the government should also recognize that while victims and ISPs might be cheapest crime avoiders, able to prevent crime more cheaply than other actors, their prevention strategies may carry broad, systemic costs, such as balkanization of the net via systems of passwords and other methods that limit access. Law enforcement must have a strong presence on the net to steer victims and ISPs away from suboptimal self-help strategies; yet at the same time, the police must stress that these entities have a duty to take self-help measures.

Fourth, instead of treating all crime as equal, law enforcement should attempt to inflict disproportionately heavy punishments upon those crimes that create the most visible, or otherwise evident, social disorder in cyberspace. Doing so will avoid complementarity problems, such as copycat crimes or crimes committed because hackers' tools are easily accessible, and will help reassure the public and industry that cyberspace is safe.

These four strategies are calculated to help set up incentives that make crime too expensive to carry out, preserve the benefits of the net, and provide computer users with the assurance that the net is at least as safe as realspace. Yet the strategies do run risks, from trenching on privacy and freedom of speech to poisoning the free flow of ideas. Those risks cannot properly be addressed in this initial Article, but doing so is a requisite component of an effective plan to combat cybercrime.

Although cyberspace has unique particularities, the lessons we have learned are not confined only to the electronic world. A central theme of this Article, for instance, is that a crucial variable for preventing crime is perpetration cost. Law can and should develop strategies to make crimes more expensive. The government currently relies on the speculative risk of imprisonment to deter wrongdoing, but a strategy focused on raising certain costs associated with the wrongdoing itself may be more effective. If the majority of criminals are gamblers, or are at least less risk-averse than others, then the law should focus on raising the fixed, ex ante monetary costs that these criminals will pay to perpetrate a crime, not on merely enhancing probabilities of jail time that criminals will tend to ignore. Deterrence may be better served by increased monetary costs on all lawbreakers rather than by traditional strategies such as raised penalties for the few criminals unlucky enough to be caught.

This Article has also noted the need for a more nuanced solution to the problem of dual-use activities and has suggested that sentencing enhancements can preserve the positive uses of a given act while attacking its negative uses. This theory of regulation applies generally, although it may be particularly useful in the area of cybercrime, the hallmark of which may be a preponderance of dual-use activities. The Article has also analyzed the benefits of other forms of regulation, such as licensing and specific exclusions. The full range of novel government tactics—from pledges to warnings, from forfeiture to suspended sentences—may also be applied profitably outside the area of cybercrime. So too, the benefits and drawbacks of using second

and third parties as cheapest crime avoiders are not limited to cybercrime but, rather, inform criminal law generally.

At issue in this treatment of cybercrime is a view of deterrence that differs substantially from that offered by economists and sociologists, one that is not fully focused on the mind of the offender at the last minute before she commits a crime. My account stresses the way in which legal rules promote deterrence in other ways, such as by encouraging products that prevent crime, building architecture that makes crime more costly to criminals, and harnessing individual conscience and public values in ways that make crime look less attractive. By manipulating variables besides legal sanctions, crime may be prevented even when criminals are not that responsive to legal sanctions.

Both realspace and cyberspace are rapidly evolving, and the way criminal law approaches these spheres today may soon be anachronistic. Still, while the approaches may need to be updated over time, the fundamental building blocks of successful anticrime strategies will remain constant. Law must strive to prevent great harm at cheap cost, and it must define costs broadly enough to include all of the negative effects of crime prevention (substitution effects, the social costs of suboptimal self-help strategies, and so on). Our system of criminal law should attempt to raise the perpetration costs of engaging in crime and should also provide enough enforcement to create the conditions under which trust flourishes and networks develop. At the same time, the government must avoid creating disincentives to utility-producing activities and must strive to surgically target harmful acts. These building blocks of criminal law apply to the brick-and-mortar world, as they do to cyberspace.